NetAlly WiFi Analizer

Руководство пользователя

Содержание

Введение

Обзор продукта

Приложение AirMagnet WiFi Analyzer - это инструмент отраслевого стандарта, предназначенный для проведения мобильной проверки, а также поиска и устранения неисправностей в корпоративных сетях Wi-Fi. Приложение AirMagnet WiFi Analyzer помогает ИТ-персоналу быстро устранять проблемы конечных пользователей, автоматически обнаруживая угрозы безопасности и уязвимости беспроводной сети. Решение позволяет администраторам сети легко тестировать и диагностировать десятки наиболее распространенных проблем с производительностью беспроводной сети, включая проблемы с пропускной способностью, проблемы с подключением, конфликты устройств и проблемы с многолучевым распространением сигналов. Приложение AirMagnet WiFi Analyzer включает в себя инструмент отчетов о соответствии, который автоматически сопоставляет собранную сетевую информацию с существующими требованиями для определения соответствия политике и отраслевым нормам.
Беспроводные локальные сети (WLAN) на основе стандарта 802.11 быстро превратились в один из важнейших активов в области корпоративных сетевых технологий. Распространению Wi-Fi во всех отраслях способствовали низкая стоимость владения и необходимость расширения существующих проводных сетей для быстро растущей базы мобильных пользователей.
Однако подобно раннему этапу развития Ethernet, скорость внедрения 802.11 опередила развитие профессиональных инструментов и методов, необходимых для правильного управления сетями WLAN. В результате специалисты по информационным технологиям и сетевой безопасности внезапно оказались в ситуации, когда им пришлось иметь дело с постоянно растущим потоком проблем сетевой безопасности и производительности, но при этом обладают они только устаревшими инструментами, изначально предназначенными для работы на проводных сетях.
В отличие от своих проводных аналогов, сети WLAN значительно более подвижны и практически не имеют физических границ. Таким образом, ИТ-специалисты и специалисты по сетевой безопасности остро нуждаются в инструментах, специально разработанных для беспроводных локальных сетей, которые помогли бы им своевременно выявлять и устранять специфические для WLAN проблемы производительности и безопасности. Именно для этого и предназначено приложение AirMagnet WiFi Analyzer.
Разработанное для того, чтобы сделать сеть WLAN такой же безопасной и надежной, как Ethernet, приложение AirMagnet WiFi Analyzer объединяет самые передовые инструменты и интеллектуальные возможности в одном мобильном анализаторе, обеспечивая правильный баланс между мониторингом, анализом и диагностикой сети. К основным функциям приложения относятся обследование и аудит объекта, устранение неполадок с подключением, а также управление безопасностью и производительностью. В основе решения лежит AirMagnet Wireless System Expert (AirWISE) – аналитический инструмент AirMagnet, на который подана заявка на патент. Он автоматически предупреждает ИТ-специалистов и сетевых специалистов о более чем 200 средствах и стратегиях атак и предоставляет контекстно-зависимый анализ и рекомендации для конкретных случаев.

Авторское право

Техническая документация AirMagnet WiFi Analyzer Pro.

AirMagnet является брендом компании NetAlly.

NetAlly
2075 Research Parkway
Colorado Springs, CO 80920

Руководство составлено в Соединенных Штатах Америки.
Версия 11.3.2, выпущенная в апреле 2020 года.

Основные особенности

Приложение AirMagnet WiFi Analyzer является самым популярным в отрасли мобильным инструментом для поиска и устранения неисправностей непосредственно на корпоративных сетях Wi-Fi. Приложение AirMagnet WiFi Analyzer помогает ИТ-персоналу разбираться с жалобами конечных пользователей и быстро устранять проблемы с производительностью, автоматически обнаруживая угрозы безопасности и другие уязвимости сети. Несмотря на компактность, приложение AirMagnet WiFi Analyzer обладает многими качествами полнофункциональной выделенной системы мониторинга беспроводной локальной сети на основе существующих политик.

Автоматическое обнаружение злоумышленников и сетевых уязвимостей

Приложение автоматически обнаруживает сотни проблем с производительностью, например, конфликты 11b/g, проблемы 802.11e и QoS, а также десятки типов беспроводных вторжений и стратегий взлома, включая мошеннические устройства, атаки типа «отказ в обслуживании», атаки по словарю, поддельные точки доступа, преднамеренные радиочастотные помехи, инструменты «Stumbler» и многое другое. Также приложение AirMagnet WiFi Analyzer предоставляет удобный инструмент поиска, который позволяет быстро отслеживать неавторизованные точки доступа и несовместимые устройства, ставящие под угрозу безопасность сети. Инструмент поиска (Find Tool) также можно использовать для выравнивания сигналов между антеннами, быстро оптимизируя прием в режиме моста прямой видимости.

Политики безопасности для блокировки

Приложение AirMagnet WiFi Analyzer позволяет устанавливать подробные политики безопасности для всех устройств в сети. Можно установить методы шифрования и аутентификации, а затем провести мониторинг своей беспроводной локальной сети, чтобы проверить все устройства на соответствие этим политикам и убедиться, что сами методы шифрования в беспроводной локальной сети работают правильно. Установите еще более высокий уровень организованной безопасности, назначив список утвержденных для клиентского доступа точек доступа и отслеживая открытые беспроводные станции, устройства ad-hoc и другие уязвимости.

Выполнение интерактивных сетевых тестов в реальном времени

Кроме автоматического обнаружения проблем приложение AirMagnet WiFi Analyzer также предоставляет набор инструментов для активного поиска и устранения неисправностей. Находясь всегда под рукой, эти инструменты помогут вам быстро выявлять такие сетевые проблемы, как радиочастотные помехи,

перегрузки трафика/инфраструктуры, сбои в работе оборудования и проблемы с подключением. Соединения можно тестировать с помощью таких традиционных инструментов, как DHCP, Ping и Traceroute, или использовать инструмент диагностики AirMagnet для пошагового просмотра процесса соединения между клиентом и точкой доступа, что позволит точно определить, где этот процесс дал сбой. Для выявления несоответствий настроек сети, покрытия, многолучевых помех, джиттера и роуминга запускайте тесты производительности точки доступа.

Непрерывный анализ помех в сети Wi-Fi

Причиной появления помех могут быть различные источники, включая воздействие со стороны других устройств Wi-Fi, так называемых «скрытых узлов» в сети и даже беспроводных устройств, не поддерживающих стандарт 802.11. Все эти составляющие помех отслеживаются и четко отображаются по каналам на экране помех (Interference) приложения AirMagnet WiFi Analyzer. Это позволяет быстро обнаруживать влияние конкурирующих устройств Wi-Fi, идентифицировать любые скрытые узлы, влияющие на канал, и отслеживать шумы в радиочастотной среде. Для еще более глубокого анализа уровня 1 и выявления источников помех, не поддерживающих стандарт 802.11, пользователи AirMagnet WiFi Analyzer PRO смогут также использовать анализатор спектра AirMagnet (AirMagnet Spectrum Analyzer).

Примечание: Анализатор спектра AirMagnet (AirMagnet Spectrum Analyzer) приобретается отдельно.

Подробный анализ пакетов и кадров

Просматривайте потоки пакетов в реальном времени для любого объекта сети Wi-Fi. Отслеживайте пакеты данных и управления в реальном времени, наблюдайте ошибки CRC, контролируйте использование, скорость пакетов, тип носителя и многие другие показатели. Просматривайте страницу декодирования в реальном времени для подробного анализа сети: приложение AirMagnet WiFi Analyzer декодирует такие наиболее популярные протоколы, как FTP, HTTP, SMTP, POP и Telnet, с расширенными параметрами фильтрации, что позволяет сосредоточиться на определенных разговорах на основе IP-адреса или номера порта.

Доступ к AirMagnet AirWISE® Expert

AirMagnet AirWISE® - это энциклопедический источник информации об угрозах и проблемах производительности при работе в среде Wi-Fi. На простом языке разъясняются все системные сигналы тревоги, в том числе описывается, почему они важны и какие шаги необходимо предпринять для устранения проблем.

Мониторинг сетей 802.11n/ac

Идентифицируйте и классифицируйте все поддерживающие 802.11n/ac устройства в сети (включая определение разницы между устройствами 802.11n, совместимыми с данным стандартом, и устройствами 802.11n, выполненными по предварительному стандарту). Приложение AirMagnet WiFi Analyzer поддерживает мониторинг каналов 20 МГц, 40 МГц и 80 МГц, а также обнаруживает и классифицирует более высокие скорости передачи данных, используемые устройствами 802.11n/ac. С помощью приложения AirMagnet WiFi Analyzer можно классифицировать и декодировать трафик Non-HT (устаревший), трафик смешанного формата HT, а также трафик VHT, и выявлять проблемы обратной совместимости с устаревшими устройствами 802.11a/b/g, работающими в том же сетевом окружении. Также можно находить неавторизованные устройства стандарта 802.11n/ac, которые часто остаются невидимыми для анализаторов, не поддерживающих стандарт 802.11n, и декодировать новые информационные элементы/типы беспроводных кадров.

Создание отчетов о соответствии

Создавайте подробные отчеты о соответствии множеству нормативных стандартов, установленных регулирующими органами в соответствующих странах. К ним относятся Sarbanes-Oxley, Basel II, EU-CRD (Cad 3), ISO 27001, FISMA, HIPAA, PCI-DSS, DoD 8100.2 и GLBA. В отчетах содержится пошаговая оценка соответствия/несоответствия каждому разделу стандарта, что позволяет выполнить работу в кратчайшие сроки. Также приложение AirMagnet WiFi Analyzer предоставляет интегрированный инструмент отчетности, который позволяет превратить сеансы анализа Wi-Fi в профессиональные настраиваемые

отчеты. Можно использовать предварительно созданные отчеты из библиотеки или создавать собственные целевые отчеты, выбирая в пользовательском интерфейсе такие необходимые элементы, как статистика радиочастот, отчеты о каналах, отчеты об устройствах или отчеты о проблемах безопасности и производительности.

Поддержка нескольких форм-факторов

Приложение AirMagnet WiFi Analyzer можно установить на различные платформы, включая ноутбуки на базе Windows, планшетные компьютеры, Apple® MacBook® Pro (только с беспроводными адаптерами на базе Atheros) и ультрамобильные персональные компьютеры (UMPC). Поддержка UMPC позволяет конечным пользователям и торговым посредникам впервые всесторонне контролировать, проверять и устранять неисправности на сети WLAN с помощью помещающегося в карман персонального компьютера. Это дает возможность свободно перемещаться по помещениям для проверки и устранения неисправностей на корпоративных сетях Wi-Fi с помощью легкого переносного решения. Приложение Wi-Fi AirMagnet Analyzer поддерживается на UMPC OQO Model 02/e2.

Поддержка стандарта беспроводной сети 802.11n/ac

Приложение AirMagnet WiFi Analyzer позволяет использовать новейшие стандарты беспроводной сети, которые дают более высокую производительность, больший радиус действия и повышенную надежность - три наиболее важных элемента современных сетей. Теперь благодаря тому, что AirMagnet поддерживает беспроводные сети 802.11n, можно отслеживать на сети трафик 802.11n/ac на каналах 20, 40 и 80 МГц, идентифицировать устройства 802.11n/ac и декодировать кадры 802.11n/ac.

Инструменты 802.11n/ac

Приложение AirMagnet WiFi Analyzer поставляется с инструментами 802.11n и 802.11ac, которые позволяют анализировать производительность беспроводной сети. Это следующее поколение беспроводных сетевых технологий, которое обеспечивает беспрецедентную пропускную способность, дальность действия и стабильность сети. Описанные ниже инструменты призваны помочь понять и устранить наиболее распространенные проблемы, с которыми вы можете столкнуться:

- Efficiency Tool (Инструмент повышения эффективности) - Протоколы беспроводной сети 802.11n и 802.11ac вносят существенные улучшения в эффективность сети WLAN как на физическом уровне (PHY), так и на уровне управления доступом к среде (MAC). Инструмент повышения эффективности Efficiency Tool призван предоставить пользователю базовые знания, необходимые для использования в полной мере всех преимуществ сетей 802.11n и 802.11ac.
- Analysis Tool (Инструмент анализа) - Инструмент анализа Analysis Tool предоставляет подробные разъяснения и анализ беспроводной сети.
- WLAN Throughput Simulator (Имитатор пропускной способности сети WLAN) - WLAN Throughput Simulator является служебной программой расчета пропускной способности, использования и полезной нагрузки (измеренных на канальном уровне 802.11) сети, узла и среды передачи при различных конфигурациях сетей и узлов. Эта утилита позволяет добавить в «виртуальный канал» и настроить до пятидесяти узлов 802.11a, 802.11b, 802.11g, 802.11n и 802.11ac. Данный инструмент применяет дополнительные параметры сети и узлов в зависимости от типа и настроек имеющихся узлов. Имитатор работает в «идеальной» среде, где предполагается, что все узлы могут «слышать» друг друга (что исключает возможность коллизий пакетов и повторных попыток передачи кадров) и что все узлы передают столько (и настолько быстро), сколько они могут (на основе их индивидуальных и общих сетевых параметров). Результат подобного моделирования предоставляет базовое измерение (в определенном смысле теоретическое) максимальной пропускной способности канального уровня, которой можно достичь в конкретной конфигурации.
- Device Throughput Calculator (Калькулятор пропускной способности устройства) - Калькулятор пропускной способности устройства представляет собой служебную программу для расчета теоретической пропускной способности устройства. Просто указывайте щелчком мыши такие параметры, как индекс MCS, SGI, полоса пропускания, максимальный размер кадра, блок ACK, наименее способное устройство и/или используемый механизм защиты. После этого AirMagnet за считанные мгновения рассчитает максимальную скорость на физическом уровне, максимальную скорость передачи данных, процент служебных данных, количество пространственных кадров и кодовую скорость модуляции. Также в виде графика, показывающего процентное соотношение кадров DIFS, преамбулы/PLCP, данных, SIFS, преамбулы/PLCP и ACK, будут отображены данные обмена кадрами 802.11.

Интеграция с беспроводной конфигурацией Windows

Приложение AirMagnet WiFi Analyzer позволяет использовать профили беспроводной связи, созданные в операционной системе Windows, и применять их напрямую с активными инструментами AirMagnet WiFi Analyzer (например, Site Survey (Обследование объекта), Performance (Производительность), Connect (Подключение), Roaming (Роуминг) и т.д.).

Практическое руководство

Приложение AirMagnet WiFi Analyzer включает в себя практическое руководство в стиле Microsoft Office Assistant, которое поможет быстрее освоить его основные функции. Руководство доступно во всех основных пользовательских интерфейсах; доступ к нему можно получить одним нажатием кнопки.

Удаленное устранение неисправностей

Существуют следующие возможности подключения к удаленным системам для дистанционного устранения неисправностей:

- Вариант 1: этот вариант подразумевает включение режима удаленной работы на компьютере, где установлено приложение AirMagnet WiFi PRO. Когда компьютер установлен в этот режим, к нему можно установить удаленное подключение с локального компьютера, на котором запущено приложение AirMagnet WiFi Analyzer PRO. Локальный компьютер переключается на удаленный адаптер для сбора данных.
- Вариант 2: можно удаленно подключиться к некоторым моделям датчика AirMagnet SmartEdge.

Системные требования

Примечание: Это минимальные системные требования. Скорость захвата и анализа пакетов зависит от производительности системы. Система с более высокой производительностью обеспечивает лучшие результаты для захвата и анализа пакетов.

Портативный компьютер/ноутбук/планшет

- Операционные системы: Microsoft® Windows 8.1 Pro/Enterprise 64-разрядная или Microsoft® Windows 10 64-разрядная.
- Процессор Intel® Core™ 2 Duo 2,00 ГГц (рекомендуется Intel® Core™ i5 или выше).
- Память 4 ГБ или больше.
- 800 МБ свободного места на жестком диске.
- Слот ExpressCard или порт USB, или адаптер беспроводной сети, поддерживаемый AirMagnet.
- При использовании нескольких адаптеров потребуется несколько слотов на компьютере. NetAlly рекомендует использовать свой многоадаптерный комплект.
- Адаптер (адаптеры) беспроводной сети, поддерживаемый AirMagnet.
- Дополнительный адаптер для анализа спектра и лицензия (требуется для просмотра данных спектра и устройств вне сети Wi-Fi; только для приложения AirMagnet WiFi Analyzer PRO). Поддерживается интеграция с AirMagnet Spectrum XT.

Примечание: Адаптер Spectrum XT выполнен в форм-факторе USB.

Apple® MacBook® Pro

- Операционные системы: MAC OS X (Leopard™) под управлением поддерживаемой операционной системы Windows (как указано в разделе «Портативный компьютер/ноутбук/планшет») с использованием Boot Camp®.
- Рекомендуется процессор Intel® Core™ 2 Duo 2,00 ГГц или выше.
- Память 4 ГБ или больше.
- 800 МБ свободного места на жестком диске.
- Внутренний адаптер WLAN Broadcom 802.11ac (модели MacBook 2013 и 2014), адаптер WLAN Airport Extreme 802.11n на базе Atheros или порт USB (в зависимости от того, что применимо).
- При использовании нескольких адаптеров потребуется несколько слотов на компьютере. NetAlly рекомендует использовать свой многоадаптерный комплект.

- Дополнительный адаптер для анализа спектра и лицензия (требуется для просмотра данных спектра и устройств вне сети Wi-Fi; только для приложения AirMagnet WiFi Analyzer PRO). Поддерживается интеграция с AirMagnet Spectrum XT.

Примечание: Адаптер Spectrum XT выполнен в форм-факторе USB.

Поддерживаемые адаптеры Wi-Fi

Для сбора данных Wi-Fi приложению AirMagnet WiFi Analyzer необходимо, чтобы на компьютере, где запущено приложение, работал поддерживаемый адаптер Wi-Fi.
Список поддерживаемых адаптеров приводится на странице https://www.netally.com/wp-content/uploads/2019/12/AMM-Preferred-Adapters.pdf.

Поддерживаемые форматы файлов

Приложение AirMagnet WiFi Analyzer поддерживает файлы следующих форматов:
.amc - собственный формат файлов AirMagnet, который позволяет воспроизводить сохраненные данные, как если бы воспроизводилось видео. Это дает возможность повторно просматривать данные в том виде, в котором они были захвачены.
.ecp - формат файлов Ethereal.
.cap - формат файлов Sniffer.
.amm - собственный формат файлов AirMagnet, используемый для поддержки записи на диск (Capture to Disk) и мультиадаптера (Multiadapter). Сохранение в этом формате возможно только при включении одной из этих функций.
.pcap - файлы, сохраненные с опцией стандарта 802.11+.

Техническая поддержка

Поддержка продуктов AllyCare

Программа AllyCare от NetAlly - это комплексная программа поддержки и обслуживания, которая предлагает расширенное покрытие для продуктов NetAlly.
Для получения дополнительной информации посетите https://www.netally.com/support/.

Связаться с нами

Звоните по бесплатному телефонному номеру в Северной Америке: 1-844-TRU-ALLY (1-844-878-2559)
Чтобы узнать дополнительные номера телефонов, посетите https://www.netally.com/contact-us/. Для заполнения веб-формы прокрутите страницу вниз и выберите свой регион; представитель компании NetAlly свяжется с вами.

Установка

Проверка комплектации продукта

Перед тем как начать, убедитесь, что в комплект поставки продукта входит следующее:
- Компакт-диск с продуктом.
- Лицензионное соглашение по программному обеспечению.
- Документ Read Me First (Прочитайте в первую очередь).
- Сертификат программного обеспечения с серийным номером и серийным ключом.
- Если был приобретен контракт на поддержку, то в поставку входит контракт на поддержку с серийным номером поддержки и серийным ключом.

Если что-либо из этого списка отсутствует или повреждено, немедленно обратитесь к авторизованному торговому посреднику AirMagnet или в службу технической поддержки AirMagnet.

Подготовка к установке программного обеспечения

Перед началом установки продукта ознакомьтесь с приведенной ниже информацией.

Проверьте системные требования

Убедитесь, что компьютер, на который планируется установить программное обеспечение, соответствует системным требованиям. Обратитесь к разделу «Системные требования».

Перед тем, как начать

Перед установкой, запуском и использованием программного обеспечения обратите внимание на следующее:
- При первом запуске программного обеспечения убедитесь, что имеется активное подключение к сети Интернет.
- Необходимо иметь права администратора на компьютере, на котором запущено программное обеспечение AirMagnet.
- Имейте в виду, что определенные настройки брандмауэра или антивирусного программного обеспечения могут мешать работе программного обеспечения AirMagnet.
- Сетевое программное обеспечение, использующее беспроводный адаптер, может вызвать конфликт с программным обеспечением AirMagnet.

Обновления продукта

Если компьютер, на котором запущено программное обеспечение, имеет активное Интернет-соединение, и доступно обновление продукта, во время запуска продукта появится диалоговое окно с уведомлением о наличии более новой версии. Нажмите Yes (Да), чтобы перейти в свою учетную запись MyAirMagnet, где можно будет получить доступ к загрузке обновления программного обеспечения. Обновление продукта будет показано в разделе Registered Products / Downloads (Зарегистрированные продукты / Загрузки) под Software Download (Загрузка программного обеспечения).
Для перехода со старой версии на новую версию продукта требуется активный контракт на поддержку. Все существующие клиенты, желающие установить более новую версию продукта, должны проверить состояние своего контракта на поддержку продукта перед началом установки.

Состояние своего контракта на поддержку можно просмотреть в разделе Registered Products (Зарегистрированные продукты) своей учетной записи MyAirMagnet. Для получения информации о контрактах на поддержку обратитесь к разделу «Техническая поддержка».

Лицензия на программное обеспечение

Для успешного запуска программного приложения необходимо установить уникальную лицензию на программное обеспечение. При первом запуске продукта будет предложено установить лицензию.

Получение лицензии на программное обеспечение

Сертификат лицензии на программное обеспечение включает серийный номер (S/N) и серийный ключ (Serial Key). При первом запуске приложения для продолжения потребуется предоставить эту информацию. Комбинация серийного номера/серийного ключа позволяет получить лицензию на программное обеспечение, совместимую с версией программного обеспечения конкретного продукта и в соответствии с имеющимся контрактом на поддержку.
После ввода серийного номера и серийного ключа будет предложено получить лицензию:

- License Download (Загрузка лицензии): Если компьютер подключен к сети Интернет, лицензию можно загрузить. В этом случае система автоматически загрузит и установит лицензию.
- Browse to License (Найти лицензию): Если лицензия доступна в вашей сети (загружена ранее), можно выбрать ее поиск. Имя файла лицензии - «серийный номер.lic».

Например: A1150-04280450.lic.

Лицензия будет скопирована в каталог продуктов AirMagnet.
Например: c:\Program Files\AirMagnet Inc\AirMagnet Laptop.

Привязка лицензии к MAC-адресу

Для каждого MAC-адреса разрешена одна лицензия на программное обеспечение. Лицензия может быть привязана к конкретному компьютеру (ноутбуку) или к съемному беспроводному адаптеру. Это обеспечивает гибкость использования продукта.
Во время установки продукта будет предложено выбрать, какой вариант использовать. В зависимости от сделанного выбора приложение автоматически захватывает MAC-адрес компьютера или адаптера.

Примечание: Если лицензия на программное обеспечение будет привязана к съемному адаптеру, в момент запуска приложения этот адаптер должен быть активен на компьютере.

Сброс MAC-адреса

Если необходимо сбросить MAC-адрес на другой компьютер или адаптер, эту операцию можно запросить, выбрав MAC Address Reset (Сброс MAC-адреса) в своей учетной записи MyAirMagnet.

Резервное копирование файла лицензии

Настоятельно рекомендуется зарегистрировать продукт, загрузить файл лицензии и сохранить его в надежном месте. Наличие резервного файла лицензии позволяет легко и в любое время переустановить приложение, если это необходимо, потому что для его установки можно просто найти нужный файл.

Установка программного обеспечения продукта

Если имеется текущий контракт на поддержку, будет загружена самая последняя версия продукта; в противном случае это будет та версия, на загрузку которой вы имеете право.

1. На странице Registered Products (Зарегистрированные продукты) своей учетной записи MyAirMagnet щелкните кнопкой мыши на загрузке программного обеспечения и запустите или сохраните файл. Если файл был сохранен, дважды щелкните кнопкой мыши на файле .exe, чтобы запустить программу установки.
2. Чтобы продолжить установку, примите условия лицензионного соглашения на программное обеспечение. Обратитесь к разделу «Лицензионное соглашение на программное обеспечение».
3. Задайте папку назначения для установки программного обеспечения. Примите по умолчанию папку Program Files или выберите другое место.
4. Для завершения установки нажмите Finish (Готово). На этом этапе можно выбрать в программе установки другую опцию или нажать кнопку Exit (Выход), чтобы закрыть программу установки.

Поддержка декодирования верхнего уровня

Приложение AirMagnet WiFi Analyzer предоставляет возможность использования стороннего инструмента декодирования для декодирования верхних уровней файлов захвата. Данную функцию можно выбрать в процессе установки продукта. Информация о лицензии приводится в разделе «Лицензия на функцию поддержки декодирования верхнего уровня».

Для установки стороннего инструмента декодирования:

1. Во время установки программного обеспечения будет предложена возможность установить 3rd Party Decodes (Сторонние декодеры). Щелкните копкой мыши на Yes (Да).

2. Чтобы продолжить установку сторонних декодеров, вы должны согласиться с лицензией GNU Library General Public License.
3. Кроме того, можно разрешить доступ к этой функции всем, кто использует компьютер.

Примечание: Если на данном этапе вы решите не устанавливать сторонние декодеры, то можете выбрать установку из приложения на вкладке Filter (Фильтр) в диалоговом окне Configuration (Конфигурация).

Регистрация продукта

Рекомендуется создать учетную запись My AirMagnet и зарегистрировать программное обеспечение AirMagnet. Регистрация приобретенного программного обеспечения дает право на бесплатную учетную запись My AirMagnet со следующими преимуществами:

- Загрузка обновлений программного обеспечения в случае их доступности.
- Доступ к документации по продукту (часто задаваемые вопросы, передовой опыт, примечания к выпуску, руководства пользователя и т.д.).
- Загрузка драйверов беспроводного адаптера.
- Доступ к техническим заметкам/официальным документам.
- Доступ к форумам AirMagnet.
- Доступ к программам обучения.

Для регистрации продукта и создания учетной записи My AirMagnet, перейдите по ссылке: https://airmagnet.netally.com/support/register_product/

Активация контракта на поддержку

Приобретенный контракт на поддержку продукта необходимо активировать.

- При первом запуске продукта: будет предложено ввести серийный номер контракта на поддержку и серийный ключ.
- Для добавления нового контракта на поддержку к существующей лицензии на программное обеспечение зарегистрируйте свой продукт. В разделе Registered Products / Downloads (Зарегистрированные продукты / загрузки) учетной записи My AirMagnet под Product Version (Версия продукта) нажмите Register Support Contract (Зарегистрировать контракт на поддержку). Будет предложено ввести серийный номер контракта на поддержку и серийный ключ.

Примечание: Серийный номер и серийный ключ контракта на поддержку не совпадают с серийным номером и серийным ключом самого продукта.

Первый запуск приложения

При первом запуске приложения нужно будет подтвердить свою лицензию и установить ее.

Метод установки лицензии

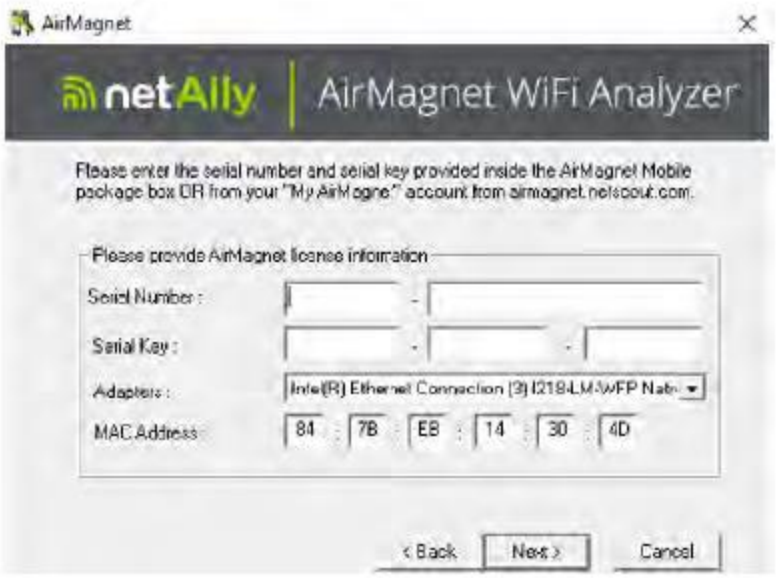
Выберите, какой метод использовать для установки лицензии на программное обеспечение:
- Download the license (Загрузить лицензию): Потребуется активное подключение к сети Интернет.
- Browse to a license (Найти лицензию): Будет предложено найти файл.

Привязка лицензии к MAC-адресу

Выберите один из двух вариантов, чтобы привязать лицензию:
- The MAC address of a computer running the application (MAC-адрес компьютера, на котором запущено приложение). Если выбран этот вариант, приложение можно будет запускать только на этом компьютере.
- The MAC address of a removable Wi-Fi adapter (MAC-адрес съемного адаптера Wi-Fi). Чтобы привязать лицензию к адаптеру Wi-Fi, тот должен быть активен на компьютере, на котором запущено приложение. Обратитесь к разделу «Подготовка к установке программного обеспечения». Если выбрать этот вариант, адаптер должен быть подключен к компьютеру, на котором запущено приложение.

Предоставление серийного номера и серийного ключа

При первом запуске программного обеспечения также потребуется предоставить действительный серийный номер и серийный ключ. Если имеется контракт на поддержку этого продукта, здесь также нужно указать его данные.

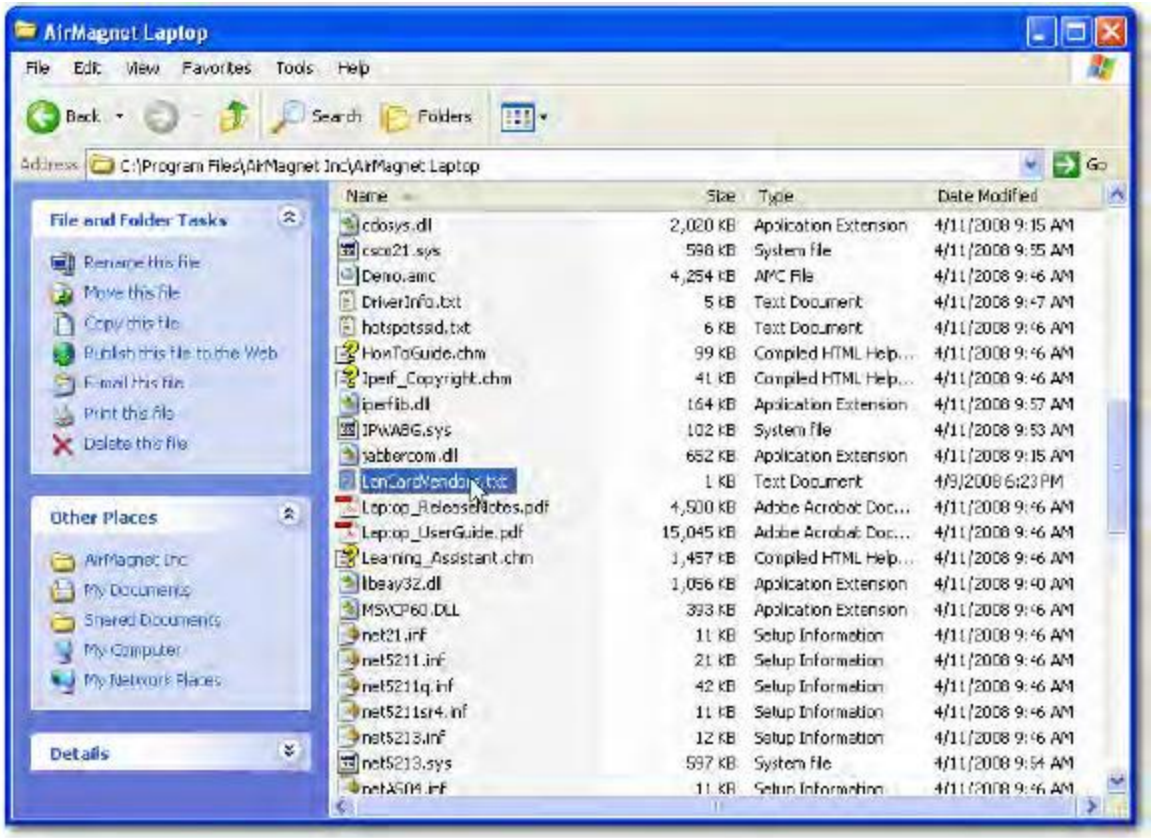


Если файл лицензии не поддерживает установленную версию продукта, появляется сообщение об ошибке Invalid License File (Недействительный файл лицензии) или This serial number is currently out of support (Этот серийный номер в настоящее время не поддерживается).
Если сообщение об ошибке появляется при попытке установить лицензию на программное обеспечение, это может происходить по одной из следующих причин:
- Ваша лицензия не поддерживает более новую версию продукта. В этом случае можно приобрести контракт на поддержку, который дает право запускать более новое программное обеспечение. Обратитесь в службу технической поддержки.
- Выбранный вами файл лицензии предназначен для другого продукта. Убедитесь, что имя файла лицензии имеет тот же серийный номер, что и серийный номер вашего продукта. Обратитесь к разделу «Подготовка к установке программного обеспечения».

Если появилось сообщение Invalid License (Недействительная лицензия) или This serial number is currently out of support (Этот серийный номер в настоящее время не поддерживается) и вы считаете, что это неверно, обратитесь в службу технической поддержки. Вам будет предложено указать серийный номер и серийный ключ для рассматриваемого продукта.

Обновление списка производителей беспроводных сетевых устройств

Во время установки приложения AirMagnet WiFi Analyzer в папку AirMagnet Wi-Fi автоматически копируется файл с именем LANCardVendors.txt.



Файл LANCardVendors.txt содержит информацию для сопоставления OUI (уникальных идентификаторов организации) в MAC-адресах сетевых устройств с именами производителей, их выпускающих. Создание пар из MAC-адреса и производителя упрощает классификацию и распознавание многочисленных сетевых аппаратных устройств, используемых в сети.

MAC-адрес (Media Access Control - управление доступом к среде), также известный как аппаратный адрес Ethernet (Ethernet Hardware Address - EHA), аппаратный адрес или адрес адаптера - это квазиуникальный идентификатор, закрепленный/назначенный сетевому адаптеру, то есть карте сетевого интерфейса (Network Interface Card - NIC). MAC-адрес - это число, которое является именем конкретного сетевого адаптера. Согласно стандарту IEEE 802 MAC-адрес состоит из шести групп из двух шестнадцатеричных цифр, разделенных двоеточием (:). MAC-адреса могут быть «глобально назначаемыми» или «локально назначаемыми». Глобально назначаемый адрес однозначно назначается устройству его производителем, и иногда его называют «зашитым адресом» (BIA). Первые три октета (в порядке передачи) MAC-адреса идентифицируют производителя, выдавшего MAC-адрес, и известны как уникальный идентификатор организации (OUI).

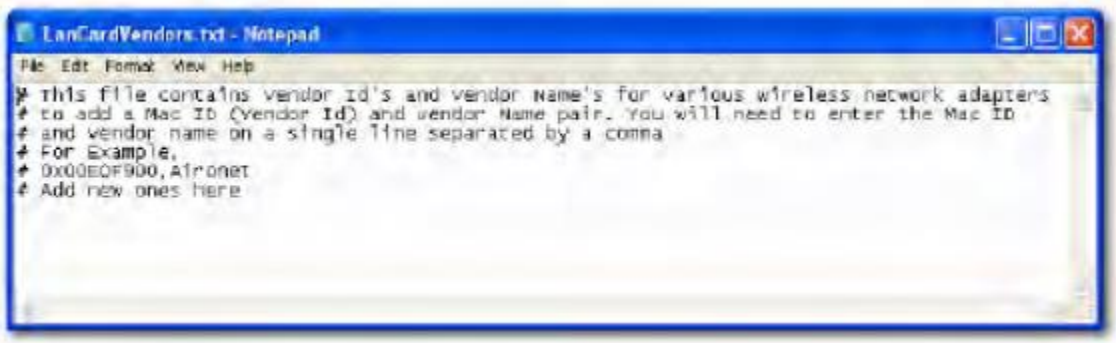
Остальные три октета назначаются этим производителем практически в любом желаемом порядке, но с учетом обеспечения уникальности. С другой стороны, локально назначаемый MAC-адрес назначается устройству администратором сети. Адреса с локальным назначением не содержат идентификатора OUI.

3 байта	3 байта
Уникальный идентификатор организации (OUI)	Конкретный контроллер сетевого интерфейса (NIC)

По умолчанию MAC-адреса всех существующих беспроводных сетевых устройств уже сопоставлены с названиями соответствующих поставщиков. Такие сопоставления отображаются на экране Start приложения AirMagnet WiFi Analyzer. AirMagnet периодически, по мере появления на рынке новых аппаратных устройств, обновляет сопоставление MAC-адресов и названий производителей, используемых в ее продуктах. Файл LANCardVendorsFile.txt предназначен исключительно для помощи пользователям, которые хотят создавать сопоставления MAC-адресов с названиями производителей самостоятельно, не дожидаясь обновления AirMagnet.

Для сопоставления MAC-адресов с названиями производителей:

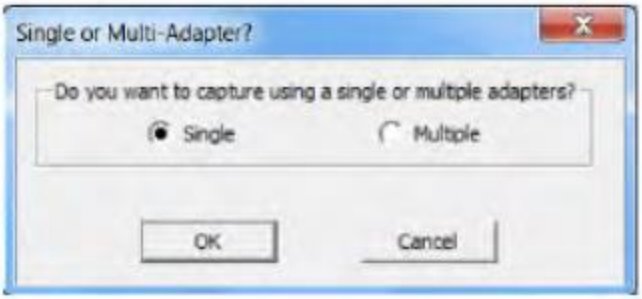
1. На портативном компьютере найдите и откройте файл LANCardVendorsFile.txt.



2. Чтобы сопоставить идентификатор OUI (в MAC-адресах) аппаратных устройств, используемых в вашей сети, с названиями соответствующих производителей, следуйте инструкциям в файле.
3. Для сохранения созданных сопоставлений щелкните кнопкой мыши на File > Save (Файл > Сохранить).
4. Закройте файл.

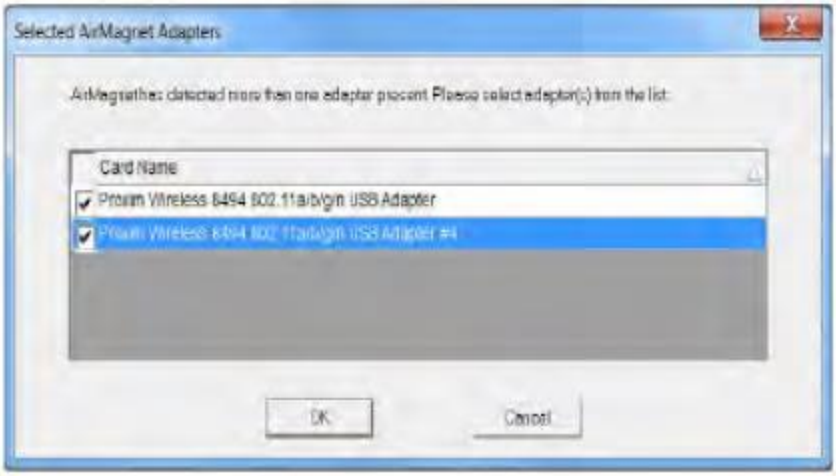
Использование нескольких беспроводных адаптеров

Если к компьютеру с приложением AirMagnet WiFi Analyzer подключено несколько беспроводных адаптеров с поддержкой AirMagnet, во время запуска приложения будет предложено выбрать адаптеры, которые следует использовать в процессе.
Поскольку приложение AirMagnet WiFi Analyzer способно поддерживать различные адаптеры с поддержкой AirMagnet, при использовании нескольких адаптеров в диалоговом окне запуска появится информация о том, какие комбинации адаптеров подходят для использования.
Для получения информации о настройке сканирования каналов обратитесь к разделу «Настройка сканирования каналов».
При обнаружении комбинации функции использования нескольких адаптеров и неподдерживаемых адаптеров:
Можно выбрать, использовать ли режим с одним или несколькими адаптерами.



Если вы выбираете режим с одним адаптером (Single), отображается диалоговое окно выбора адаптера.

Если выбран режим с несколькими адаптерами (Multiple), появится диалоговое окно для выбора необходимых адаптеров.



Если все обнаруженные адаптеры поддерживают функцию использования нескольких адаптеров:

Для одновременного использования можно указать до трех адаптеров. При работе в режиме с несколькими адаптерами каждый активный беспроводный адаптер работает на одном канале, что позволяет одновременно отслеживать весь трафик на выбранных каналах.

Системная навигация

Запуск приложения AirMagnet Wi-Fi Analyzer

На рабочем столе портативного компьютера нажмите Start (Пуск) > All Programs (Все программы) > AirMagnet > AirMagnet WiFi Analyzer.
Появится экран Start приложения AirMagnet WiFi Analyzer.

Основные компоненты пользовательского интерфейса

Пользовательский интерфейс состоит из основных компонентов, описанных в следующей таблице:

Элемент	Описание
Панель заголовка 	На находящейся в левой верхней части экрана панели заголовка отображается информация о приложении. Когда приложение работает в режиме записи в реальном времени, будет показано «Live Capture» с названием текущего профиля в скобках, например, как в данном случае [Sunnyvale, CA]. При воспроизведении файла трассировки AirMagnet (.amc) будет показано имя файла и ход воспроизведения файла в процентах.
	Примечание: По умолчанию анализатор WiFi автоматически присваивает файлу трассировки (.amc) имя по дате сохранения файла, если вы не измените или не переименуете его. Например, файл трассировки, сохраненный в пятницу, 29 февраля 2008 года, называется «Friday, February 29, 2008.amc».
Панель меню 	Расположенная прямо под строкой заголовка панель меню содержит инструменты и меню для работы с приложением.
	Примечание: В то время, как некоторые меню или инструменты применимы ко всем основным экранам, другие доступны только на определенных экранах.
Панель навигации 	Панель навигации расположена в нижнем левом углу экрана прямо над индикатором сканирования каналов Она содержит кнопки навигации, позволяющие перемещаться по основным экранам приложения.
Индикатор сканирования каналов 	Индикатор сканирования каналов расположен в нижнем левом углу экрана прямо под панелью навигации. Он показывает в реальном времени диапазон радиочастот 802.11 и сканируемые каналы. Каналы, на сканирование которых настроено приложение, отображаются здесь поочередно, в зависимости от частоты выбранного частотного диапазона. Однако если приложение настроено на сканирование одного определенного канала, то здесь будет отображаться только этот канал. Кроме того, когда на экране Channel (Канал) выбран определенный канал, то здесь будет отображаться только этот канал.
Индикатор состояния буфера 	Расположенный в правом нижнем углу экрана прямо напротив индикатора сканирования каналов индикатор состояния буфера показывает состояние системной буферной памяти в процентах. Как только значение на индикаторе достигнет 100%, все данные из буферной памяти будут удалены и по мере захвата новых данных накопление начнется заново. Этот процесс повторяется бесконечно, пока приложение работает в режиме захвата данных в реальном времени.
View Filter (Фильтр просмотра)	Расположенная вверху вдоль правого края экрана панель View Filter (Фильтр просмотра) позволяет выбрать тип данных, которые представляют наибольший интерес или беспокойство.
How-to-Guide (Практическое руководство)	Расположенная непосредственно под панелью View Filter (Фильтр просмотра) вверху вдоль правого края экрана панель How-to-Guide (Практическое руководство) предоставляет интерактивную помощь, позволяющую пользователю ознакомиться с некоторыми основными функциями приложения.
 Захват на диск	Иконка «диска» в правом нижнем углу экрана приложения отображается, когда включена функция Capture to Disk (Захват на диск).

Панель навигации

Панель навигации расположена в нижнем левом углу пользовательского интерфейса приложения AirMagnet WiFi Analyzer. Она позволяет перейти к любому из основных экранов нажатием соответствующей кнопки. На рисунке ниже показана панель навигации по умолчанию.

Как видно из рисунка выше, панель навигации содержит следующие кнопки:

Кнопка навигации	Описание
Start (Начальный) 	Позволяет открыть начальный экран (Start), на котором можно быстро просмотреть состояние сети.
Channel (Канал) 	Позволяет открыть экран Channel (Канал), который дает возможность сосредоточиться на проблемах, связанных с конкретным каналом.
Interference (Помехи) 	Позволяет открыть экран Interference (Помехи), на котором можно провести подробный анализ различных источников радиочастотных помех в сети.
Infrastructure (Инфраструктура) 	Позволяет открыть экран Infrastructure (Инфраструктура), на котором можно провести подробный анализ всех устройств, обнаруженных в сети.
Roaming Analysis (Анализ роуминга) 	Позволяет открыть экран Roaming Analysis (Анализ роуминга), который дает возможность устранять проблемы с роумингом.
AirWISE 	Позволяет открыть экран AirWISE, на котором можно сосредоточить свое внимание на анализе различных тревог, связанных с безопасностью и/или производительностью, появившихся в сети.
Top Traffic Analysis (Анализ трафика по максимальным показателям) 	Позволяет открыть экран Top Traffic Analysis (Анализ трафика по максимальным показателям), на котором можно визуально проанализировать самые срочные проблемы на сети в определенной категории.
Reports (Отчеты) 	Позволяет открыть экран Reports (Отчеты), на котором можно просматривать различные отчеты по умолчанию о сетевых данных, а также создавать собственные книги отчетов.
Decodes (Декодирование) 	Позволяет открыть экран Decodes (Декодирование), на котором можно декодировать различные пакеты, захваченные в беспроводной сети или вокруг нее.
Wi-Fi Tools (Инструменты Wi-Fi) 	Позволяет открыть экран Wi-Fi Tools (Инструменты Wi-Fi), содержащий более десятка мощных, простых в использовании инструментов для поиска и устранения неисправностей в сети

View Filter (Фильтр просмотра)

Вкладка View Filter (Фильтр просмотра), расположенная в верхней правой части пользовательского интерфейса AirMagnet WiFi Analyzer, предоставляет легкодоступные средства фильтрации отображаемых данных. Для получения доступа к различным параметрам фильтра наведите курсор мыши на вкладку, чтобы развернуть панель View Filter.

Панель View Filter (Фильтр просмотра) автоматически сворачивается при щелчке кнопкой мыши в любой области за ее пределами. Чтобы закрепить панель и оставить ее видимой, щелкните кнопкой мыши на иконке чертежной кнопки в правом верхнем углу экрана.

Применение фильтров

Панель View Filter (Фильтр просмотра) содержит четыре вкладки: Channel (Канал), SSID (Идентификатор SSID), Device (Устройство) и AirWise, на каждой из которых представлен определенный тип фильтров. Фильтрацию можно осуществлять по любой из четырех категорий или любой их комбинации. По умолчанию все фильтры отключены. Если необходимо включить определенную категорию фильтров, сначала установите метку в соответствующем поле в верхней части этой панели. Затем нужно щелкнуть кнопкой мыши, чтобы открыть вкладку соответствующего фильтра ниже, и выбрать записи для фильтрации, то есть каналы, SSID, устройства или тревоги AirWISE. Затем нужно сделать индивидуальный выбор желаемых объектов или использовать кнопку Check All (Проверить все). Наконец, для активации фильтров необходимо нажать кнопку Apply (Применить).

Вкладка Channel (Канал)

Фильтр Channel (Канал) позволяет задавать каналы, для которых на экране будут отображаться данные. Этот выбор отличается от изменения настроек сканирования каналов (обратитесь к разделу «Настройка параметров сканирования каналов») с помощью функции View Filter (Фильтр просмотра), вы просто изменяете данные, которые будут отображаться, а не данные, которые фактически обрабатываются. Другими словами, приложение AirMagnet WiFi Analyzer будет продолжать отслеживать те каналы, в полях которых не стоят метки, но не будет отображать данные от них, пока не будет отключен фильтр.

Вкладка SSID (Идентификатор SSID)

Фильтр SSID позволяет отображать данные для конкретных идентификаторов сети (SSID). Как и в случае фильтрации каналов, данная настройка влияет только на отображение данных. После отключения фильтра на экране также появятся данные, обнаруженные от других идентификаторов SSID.

Вкладка Device (Устройство)

Фильтр Device (Устройство) позволяет задавать устройства, которые будут отображаться на экране. Например, можно отфильтровывать устройства, которые были неактивны в течение определенного периода времени, или те, уровень сигнала которых упал ниже определенного значения.

Вкладка AirWISE

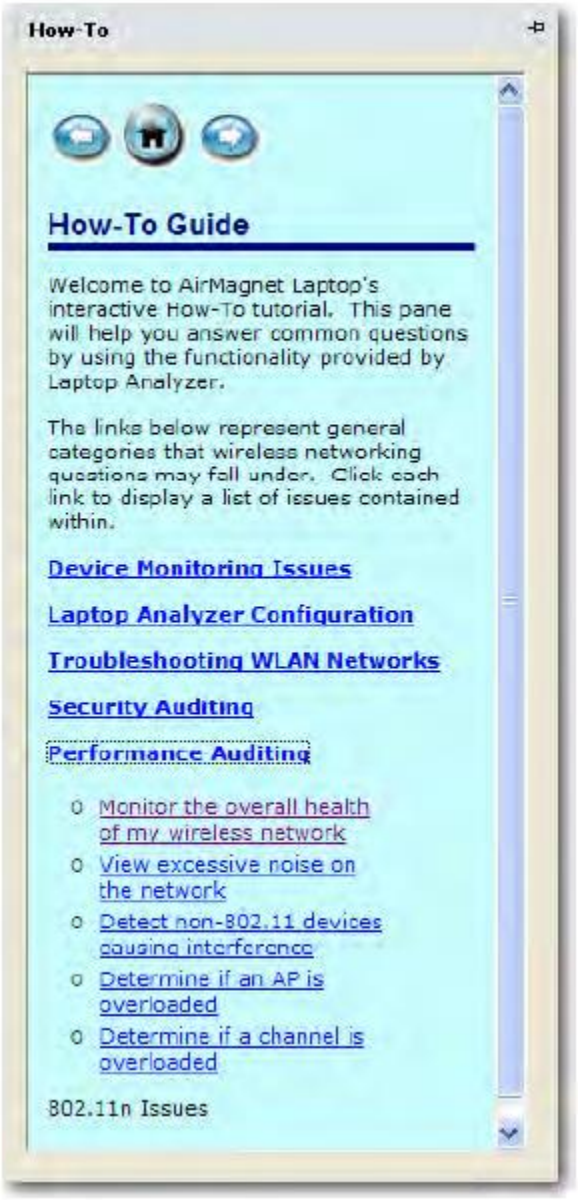
Фильтр AirWISE позволяет задавать тревоги, которые будут отображаться на экране; отображение зависит от указанного вами уровня серьезности. Это позволит сосредоточить большее внимание на сигналах тревоги, которые вам более интересны.

Для использования View Filter (Фильтр просмотра):

1. В правом верхнем углу экрана нажмите кнопку View Filter (Фильтр просмотра). Откроется панель View Filter.
2. Чтобы закрепить панель View Filter (Фильтр просмотра) в правой части экрана, щелкните кнопкой мыши на иконке канцелярской кнопки (указывающей влево).
3. Чтобы сузить круг данных, отображаемых на экране, используйте представленные на панели параметры.
4. Чтобы закрыть панель View Filter (Фильтр просмотра), щелкните кнопкой мыши на иконке канцелярской кнопки (направленной вниз).

How-To Guide (Практическое руководство)

Расположенная в правом верхнем углу экрана кнопка How-To Guide (Практическое руководство) позволяет пользователю получить контекстно-зависимую помощь. Это особенно важно новым пользователям для быстрого начала работы с приложением AirMagnet WiFi Analyzer. Ниже на рисунке показана главная страница практического руководства.

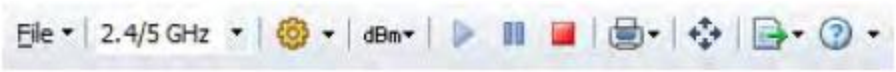


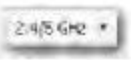
Для использования практического руководства:

1. Щелкните кнопкой мыши на How-To в правом верхнем углу экрана.
2. Чтобы закрепить панель How-To в правой части экрана, щелкните кнопкой мыши на иконке канцелярской кнопки.
3. Чтобы развернуть любую интересующую ссылку, щелкните на ней кнопкой мыши.
4. Щелкните кнопкой мыши на интересующей записи, чтобы узнать, как ее использовать.
5. По завершении щелкните кнопкой мыши на канцелярской кнопке, чтобы закрыть практическое руководство.

Панель инструментов

В верхней части экрана приложения AirMagnet WiFi Analyzer находится панель инструментов, содержащая набор кнопок и разворачивающихся списков, которые предоставляют инструменты для использования программы. Хотя некоторое содержимое панели инструментов может быть доступно только на определенных экранах, основные инструменты остаются неизменными на всех основных экранах.



Элемент	Описание
Меню File (Файл) 	В меню File (Файл) доступны следующие команды: • Open (Открыть): Позволяет открыть диалоговое окно Open (Открыть), в котором можно найти и открыть файл в формате .amc, .ecp или .cap. • Close (Закрыть): Позволяет закрыть файл, открытый в данный момент на экране. • Save (Сохранить): Позволяет сохранить захваченные приложением данные в виде файла в любом из поддерживаемых форматов. Смотрите Open (Открыть) выше. • Save As (Сохранить как): Позволяет сохранить файл, открытый в данный момент на экране, с другим именем или форматом. • Configure (Настроить): Позволяет открыть диалоговое окно AirMagnet Configuration (Конфигурация AirMagnet), в котором можно установить или изменить настройки приложения. • Policy Management (Управление политиками): Позволяет открыть экран управления политиками AirMagnet (AirMagnet Policy Management), где можно создавать или изменять профили политик для своей сети. • Operation Mode (Режим работы): Позволяет открыть диалоговое окно AirMagnet Operation Mode (Режим работы AirMagnet), в котором можно переключаться между режимом анализатора Wi-Fi AirMagnet и режимом удаленного анализатора Wi-Fi AirMagnet. • Connect To (Подключиться к): Позволяет открыть диалоговое окно входа в систему, которое дает возможность подключиться либо к удаленному анализатору Wi-Fi AirMagnet (другой портативный компьютер), либо к датчику AirMagnet. • Disconnect (Разъединить): Позволяет отключить приложение от портативного компьютера, работающего в режиме удаленного анализатора или датчика AirMagnet. • Recent Files (Последние файлы): Отображает список недавно открытых файлов. • Reset (Сброс): Данная опция позволяет удалить все собранные данные из буфера, эффективно перезапуская приложение AirMagnet WiFi Analyzer. • Exit (Выход): Позволяет закрыть приложение.
Band (Диапазон) 	Выберите диапазон, в котором хотите провести сканирование, из следующих вариантов диапазонов для 802.11. Доступные параметры соответствуют спецификации протокола 802.11 активного адаптера Wi-Fi (a/b/g/n/ac). • 2,4 ГГц (для каналов 802.11b/g/n) • 5 ГГц (для каналов 802.11a/n/ac) • 2,4/5 ГГц (для 802.11a/b/g/n/c) • 4,9 ГГц

Configure (Настроить) 	В разворачивающемся меню кнопки Configure (Настроить) находятся две опции: Configure… (Настроить) и Policy Management… (Управление политиками). Примечание: Щелчок мышью на этой кнопке напрямую открывает диалоговое окно AirMagnet Config; нажатие направленной вниз стрелки разворачивает меню, в котором показаны две опции.
Toggle Percentage or dBm (Переключение между процентами и дБм) 	Данная кнопка позволяет отображать данные на экране в процентах или в дБм.
Live capture (Захват в реальном времени) 	Эти кнопки позволяют управлять режимом захвата в реальном времени данного приложения. Слева направо располагаются кнопки «Начать захват в реальном времени», «Приостановить захват в реальном времени» и «Остановить захват в реальном времени». Примечание: Кнопка приостановки захвата в реальном времени применяется только к экрану Decodes (Декодирование).
View Reports (Просмотреть отчеты) 	Кнопка View Reports (Просмотреть отчеты) позволяет просматривать отчеты на основе данных на текущем экране и настраивать параметры принтера.
Full Screen (Полноэкранный) 	Кнопка Full Screen (Полноэкранный) позволяет переключаться между полноэкранным и обычным режимами просмотра каждого из экранов с вкладками.
Dashboard (Панель мониторинга) 	Кнопка Dashboard Selection (Выбор панели мониторинга) позволяет настраивать панель мониторинга, выбирая доступные диаграммы и таблицы из списка.
Easy View (Легкий просмотр) 	Кнопка Easy View (Легкий просмотр) позволяет открыть разворачивающееся меню, содержащее предварительно настроенные варианты просмотра, и выбрать из них подходящий.
Import/Export (Импортировать/ Экспортировать) 	Кнопка Import-Export (Импортировать/Экспортировать) позволяет импортировать или экспортировать ACL (Список контроля доступа), а также некоторые важные данные, захваченные приложением.
Help (Справка) 	В разворачивающемся меню кнопки Help (Справка) содержатся три опции: • Contents (Содержание): Позволяет открыть онлайн-справку приложения AirMagnet WiFi Analyzer. • About (О программе): Позволяет открыть диалоговое окно About AirMagnet (О AirMagnet), в котором содержится важная информация об этом приложении. • Check update (Проверить наличие обновления): Позволяет проверить наличие обновлений программного обеспечения.

Экран Start (Начальный)

Об экране Start

Экран Start приложения AirMagnet WiFi Analyzer является панелью мониторинга вашей беспроводной локальной сети. На него загружается исчерпывающая обобщенная информация о качестве радиосигнала, сетевой инфраструктуре, состоянии безопасности и производительности, а также передаче кадров в среде беспроводной локальной сети. На начальный экран можно попасть при запуске программы или, если вы находитесь на другом экране, щелкнув кнопкой мыши на 

на панели навигации. Экран Start приложения AirMagnet WiFi Analyzer показан на рисунке ниже.

По умолчанию приложение AirMagnet WiFi Analyzer запускается в режиме захвата данных в реальном времени, о чем свидетельствует надпись Live Capture в строке заголовка. На экране Start можно легко перейти к любому конкретному каналу, компоненту WLAN (например, точке доступа или клиентской станции) или тревоге безопасности или производительности для получения дополнительной информации или проведения анализа.

Панель мониторинга WiFi

Удобный в использовании интерфейс панели мониторинга приложения AirMagnet WiFi Analyzer позволяет получить быстрый обзор трафика в беспроводной среде. По умолчанию на экране Start отображается интерфейс панели мониторинга, обеспечивающий всесторонний обзор трафика. Он представляет собой мгновенный снимок общего состояния сети без необходимости разбираться в деталях. Однако возможность покопаться в деталях сохраняется, достаточно щелкнуть кнопкой мыши на нужной статистике. Доступны следующие сводные статистические данные высокого уровня:

- Channel Utilization (Использование канала)
- Channel Wi-Fi Interference (Помехи в канале Wi-Fi)
- Top Talkers (Самые активные устройства)
- Top SSIDs by Utilization (Ведущие SSID по использованию)
- Active Device Count (Количество активных устройств)

- TOP APs Based on Active Association (Ведущие точки доступа по количеству активных подключений)
- Authorized vs. Rogue Devices (Авторизованные и неавторизованные устройства)
- AP Security Settings (Настройки безопасности точки доступа)
- Top APs by Security Alarms (Ведущие точки доступа по тревогам безопасности)
- Top APs by Performance Alarms (Ведущие точки доступа по тревогам производительности)
- Device Operating Mode (Режим работы устройства)
- Top Ad-Hoc (Ведущие устройства Ad-Hoc)

Доступ к панели мониторинга можно получить в любое время, щелкнув кнопкой мыши на вкладке Dashboard, расположенной в верхней части экрана Start.
Щелкая кнопкой мыши на различных диаграммах панели мониторинга можно переходить к соответствующим экранам пользовательского интерфейса приложения AirMagnet WiFi Analyzer. Показанные диаграммы можно настраивать с помощью кнопки Dashboard Selection (Выбор панели мониторинга) на панели инструментов.

Панель меню экрана Start

Панель меню на экране Start (смотрите рисунок ниже) в дополнение ко всем обычно используемым опциям меню и инструментам содержит некоторые инструменты, которые используются только на этом экране. В этом разделе описываются инструменты, относящиеся только к экрану Start.

Панель меню на экране Start содержит следующие инструменты, которые используются только на этом экране. Они представлены иконками, отображаемыми в левой части панели меню (отмечены внутри красного прямоугольника). Название любого из этих инструментов можно узнать на экране подсказок, который автоматически всплывает при наведении курсора мыши на любой из них.

Инструмент текстового поиска

Инструмент текстового поиска позволяет легко найти узел по имени устройства, группе точек доступа, MAC-адресу или идентификатору SSID в разделе Device Data (Данные устройств) на экране Start. Просто введите критерии поиска в этом поле и нажмите кнопку (Найти на этом экране). Для продолжения поиска следующего устройства, отвечающего критерию, нажмите кнопку повторно.

Кнопка быстрого просмотра Easy View

Кнопка Easy View позволяет открыть разворачивающееся меню, содержащее предварительно настроенные опции просмотра. Можно выбрать:

- View by SSID (Просмотр по SSID) – Данная опция позволяет отсортировать все устройства в разделе Device Data (Данные об устройстве) по идентификатору SSID.
- View by Device (Просмотр по устройствам) – Данная опция группирует все устройства по имени устройства. Это особенно полезно, если имеется несколько устройств с одним и тем же именем.
- View by Media Type (Просмотр по типу среды) - Устройства группируются по типам среды: сначала отображаются устройства 802.11a, затем 11b, 11g, 11n, 11ac. Если устройства используют другой тип среды (например, FCC 4,9 ГГц), то отображаются только в том случае, если ваша карта поддерживает этот режим.
- View by Channel (Просмотр по каналу) – Данная опция сортирует устройства по каналу, на котором они обнаружены.
- View by Node Type (Просмотр по типу узла) – Данная опция (по умолчанию) позволяет сортировать все устройства по их типу (то есть точки доступа AP, станции STA или станции Ad-Hoc).
- View by 802.11n and ac (Просмотр по 802.11n и ac) – Данная опция позволяет просматривать только активные в настоящее время устройства 802.11n и 802.11ac.

Примечание: Данная опция отображается только в том случае, если используется поддерживаемый адаптер 802.11n.

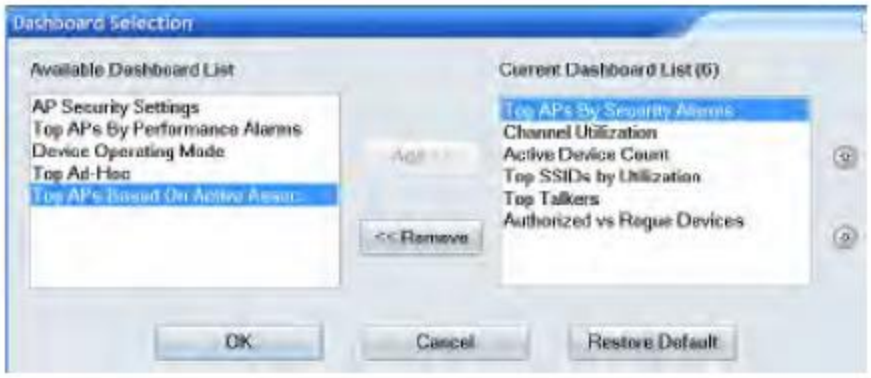
- Advanced (Расширенный) – Данная опция позволяет настроить свой способ сортировки устройств. После выбора этой опции над панелью Device Data (Данные устройства) появится новое серое поле. В это поле можно перетащить заголовки столбцов, чтобы задать древовидную структуру сортировки. Например, если необходимо сначала отсортировать по типу, затем по каналу, а затем по имени устройства, перетащите в серую область сначала заголовок столбца Type (Тип), затем заголовок Channel (Канал) и, наконец, заголовок Device (Устройство). Устройства будут отсортированы соответственно. Чтобы удалить заголовок из своего дерева, просто перетащите его ниже, обратно в заголовки столбцов.

Кнопки OK/R

Кнопки OK и R рядом с разворачивающемся меню Easy View позволяют щелчком мышью на соответствующей кнопке пометить выбранное устройство как авторизованное или неавторизованное. Просто выберите интересующее устройство на панели Device Data (Данные устройства) и щелкните кнопкой мыши на кнопке состояния (OK или R), которое хотите использовать. Изменения немедленно отразятся в столбце ACL (Список контроля доступа) на панели Device Data (Данные устройства).

Кнопка выбора панели мониторинга

Кнопка выбора панели мониторинга (Dashboard Selection) позволяет настраивать панель мониторинга путем выбора из списка доступных диаграмм и таблиц. Выберите диаграммы и таблицы в списке доступных средств мониторинга (Avaliable Dashboard List) и нажмите кнопку Add (Добавить). Нажатие кнопок в диалоговом окне добавления и удаления изменяет выбор отображаемой в настоящее время высокоуровневой статистики. Также имеется кнопка Restore Default (Восстановить по умолчанию), которая позволяет восстановить выбранный список элементов по умолчанию.



Кнопки Add (Добавить) и Remove (Удалить) для настройки панели мониторинга

Кнопка всплывающей подсказки

Данная кнопка позволяет получить справку в виде всплывающей подсказки. При включении кнопка отображается в квадратной рамке.

Кнопка полноэкранного изображения

Данная кнопка позволяет переключаться между полноэкранным и обычным режимами просмотра на каждом из экранов с вкладками.

Меню правой кнопкой мыши на экране Start

Экран Start, как следует из его названия, является отправной точкой для выявления и устранения проблем беспроводной сети. В него загружается большой объем данных, собранных приложением AirMagnet WiFi Analyzer с момента начала каждого сеанса. Для полного понимания и использования всех преимуществ разнообразных функций, показанных на этом экране, некоторые части экрана Start оснащены меню, вызываемым правой кнопкой мыши, которое позволяет сразу же перейти к определенному действию.
Далее разъясняются составные части экрана Start, имеющие контекстное меню, а также содержимое каждого из этих контекстных меню.

RF Signal Meter (Измеритель радиочастотного сигнала)

Это вызываемое щелчком правой кнопкой мыши меню содержит параметры для установки или сброса высшей точки (High Water Mark) в измерителе радиочастотного сигнала. Все, что нужно сделать, это щелкнуть правой кнопкой мыши в любом месте измерителя сигнала и выбрать опцию во всплывающем меню.

Данное контекстное меню имеет следующие опции:

- Set High Water Mark (Установить высшую точку) – Позволяет открыть диалоговое окно High Water Mark Setting (Установка высшей точки), в котором можно выбрать частоту сброса.

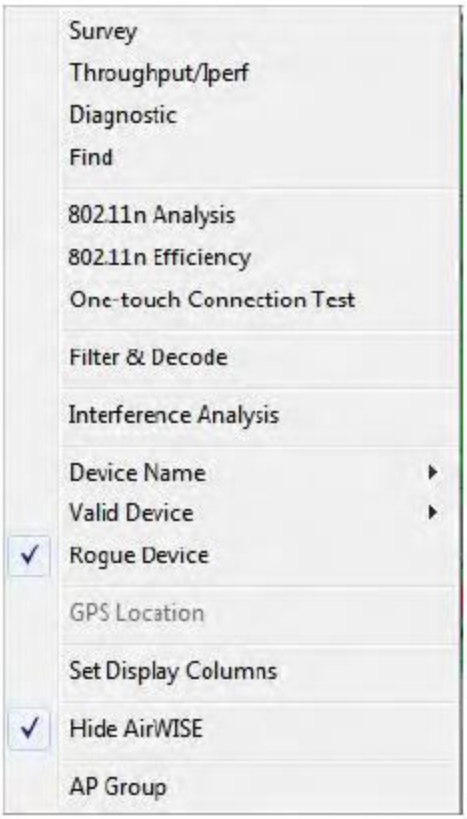
- Never Reset (Никогда не сбрасывать) - Позволяет приложению AirMagnet WiFi Analyzer никогда не сбрасывать высшую точку.

- Auto Reset with 5 sec. (Автоматический сброс через 5 секунд) - Позволяет приложению AirMagnet WiFi Analyzer сбрасывать высшую точку каждые пять секунд.
- Auto Reset with 10 sec. (Автоматический сброс через 10 секунд) - Позволяет приложению AirMagnet WiFi Analyzer сбрасывать высшую точку каждые 10 секунд.
- Reset Now (Сбросить сейчас) – Позволяет сбросить высшую точку в момент выбора этой опции.

Панель Live Network Data (Сетевые данные в реальном времени)

Это вызываемое щелчком правой кнопкой мыши меню содержит инструменты для решения проблем, связанных с устройствами, отображаемыми на экране Start. Некоторые инструменты дают возможность работать прямо с экрана, в то время как другие позволяют одним нажатием кнопки легко переходить на другие экраны.

Примечание: Перечень доступных опций зависит от типа среды на выбранном устройстве. Например, устройство 802.11n предоставляет опцию 802.11n Efficiency (Эффективность 802.11n), в то время как устройство 802.11ac предоставляет опцию 802.11ac Efficiency (Эффективность 802.11ac).



Это вызываемое щелчком правой кнопкой мыши меню имеет опции, описанные в следующей таблице:

Опция	Описание
Survey (Обследование)	Позволяет открыть экран WiFi Tools > RF > Site Survey (Инструменты WiFi > Радиочастотные > Обследование объекта).
Throughput/Iperf (Пропускная способность/Iperf)	Позволяет открыть экран WiFi Tools > Additional Tools > Throughput/Iperf (Инструменты WiFi > Дополнительные инструменты > Пропускная способность/Iperf).
Diagnostic (Диагностика)	Позволяет открыть экран WiFi Tools > Connection > Diagnostic (Инструменты WiFi > Подключение > Диагностика).
Find (Найти)	Позволяет открыть экран WiFi Tools > Additional Tools > Find (Инструменты WiFi > Дополнительные инструменты > Найти).
Analysis 802.11 n/ac (Анализ 802.11n/ac)	Позволяет открыть экран 802.11n or 802.11ac Tools > Analysis (Инструменты 802.11n или 802.11ac > Анализ) в зависимости от типа среды устройства.

802.11n/ac Efficiency (Эффективность 802.11n/ac)	Позволяет открыть экран 802.11n or 802.11ac Tools > Efficiency (Инструменты 802.11n или 802.11ac > Эффективность) в зависимости от типа среды устройства.
One-touch Connection Test (Тест подключения в одно касание)	Позволяет открыть экран WiFi Tools > Connection > One-touch Connection Test (Инструменты WiFi > Подключение > Тест подключения в одно касание).
Filter & Decode (Фильтр и декодирование)	Позволяет открыть экран Decodes (Декодирование).
Interference Analysis (Анализ помех)	Позволяет открыть экран Interference (Помехи).
Device Name (Имя устройства)	Позволяет открыть всплывающее меню, которое содержит опции управления способом отображения или идентификации устройств на экране.
Valid Device (Легитимное устройство)	Позволяет открыть всплывающее меню, которое дает возможность назначить выбранное (выделенное) устройство в группу ACL (Список контроля доступа).
Rogue Device (Неавторизованное устройство)	Позволяет изменить статус ACL (Список контроля доступа) устройства с легитимного устройства на неавторизованное.
GPS Location (Местоположение по GPS)	Позволяет открыть экран AP GPS Location (Местоположение точки доступа по GPS), на котором можно указать такие GPS-параметры точки доступа, как широта, долгота, высота над уровнем моря, высота антенны и т.д.
	Примечание: Чтобы данный параметр стал доступным, необходимо поставить метку в поле Enable GPS Port (Включить порт GPS) и выполнить настройку GPS.
	Set Display Column (Установить столбец отображения) – Позволяет открыть диалоговое окно Field Chooser (Выбор поля), которое дает возможность решить, какие данные (столбцы) должны отображаться на экране Start. Show/Hide AirWISE (Показать/скрыть AirWISE) - Позволяет показать или скрыть панель AirWISE в нижней части экрана Start. AP Group (Группа точек доступа) – Позволяет открыть экран AirMagnet Configuration > AP Grouping (Настройка конфигурации AirMagnet > Группирование точек доступа).

Вид с вкладками

Данные в правом верхнем углу экрана сгруппированы по вкладкам – Dashboard (Панель мониторинга), All Devices (Все устройства), AP (Точка доступа), STA (Станция) и Ad-hoc (Станция Ad-hoc). На вкладках All Devices/AP/STA/Ad-hoc представлены подробные данные об устройстве (обратитесь к разделу Device Data (Данные устройства)), а на вкладке Dashboard (Панель мониторинга) представлен высокоуровневый сводный отчет о состоянии сети WLAN.

Измеритель радиочастотного сигнала

В верхней левой части экрана Start находится измеритель радиочастотного сигнала, который предоставляет обзор качества радиочастотного сигнала на всех доступных каналах, каждый из которых представлен индивидуальным вертикальным столбцовым индикатором. Столбцы индикатора имеют функцию высшей точки, которая отображает самый высокий уровень радиочастотного сигнала, достигнутый каждым каналом в течение заданного пользователем интервала (настраивается на вкладке General (Общие) диалогового окна AirMagnet Configuration (Настройка конфигурации AirMagnet)).

Эта часть экрана состоит из двух разделов: в верхнем отображается диапазон 2,4 ГГц и все доступные каналы 802.11b/g/n, а в нижнем диапазон 5 ГГц и все доступные каналы 802.11a/n/ac.

Примечание: Имейте в виду, что доступные в двух частотных диапазонах каналы различаются, и что количество доступных каналов для одного и того же диапазона также может отличаться в разных странах/регионах мира, в зависимости от нормативных правил, действующих в регионе текущего использования приложения AirMagnet WiFi Analyzer.

Коды качества радиочастотного сигнала

Как видно на экране, индивидуальные индикаторы каналов имеют цветовую кодировку; цвета (зеленый, коричневый и красный) изменяются динамически, отражая колебания качества радиосигнала в сети в режиме реального времени. Чтобы узнать условия радиочастотной среды на канале, наведите курсор мыши на любой интересующий вас канал. На мгновение появится всплывающий экран с кратким описанием условий на выбранном канале.

Для каналов 2,4 ГГц (802.11b/g/n) качество радиочастотного сигнала имеет следующую цветовую маркировку:

- Зеленый: Показывает, что на канале обнаруживаются точки доступа (AP) и/или станции (ST). Если неназначенный канал горит ярко-зеленым цветом, это может указывать на то, что имеются радиочастотные сигналы, поступающие от точек доступа соседнего предприятия или от некоторых других неизвестных источников, возможно, от неавторизованных точек доступа. В этом случае следует принять меры по поиску источников всех неопознанных радиочастотных сигналов.
- Коричневый: Показывает, что на канале обнаруживаются межканальные помехи или станции, передающие сигналы зондирования. Межканальные помехи распространены в сети 802.11, потому что каналы 802.11 имеют тенденцию к перекрыванию друг друга. Следовательно, точка доступа, передающая радиочастотные сигналы на канале 2, неизбежно вызовет заметные помехи на каналах

1 и 3. Именно поэтому точкам доступа должны быть назначены неперекрывающиеся каналы. Например, если имеется три точки доступа и доступны каналы с 1 по 11, можно назначить точкам доступа каналы 1, 6 и 11 соответственно, чтобы свести к минимуму вероятность возникновения межканальных помех.

- Красный: Указывает на то, что на канале обнаружены шумы. Если имеются беспроводные телефоны диапазона 2,4 ГГц, веб-камеры, микроволновые печи или аналогичные устройства, работающие в том же частотном спектре, можно увидеть уровень шума (красная полоса) выше 10% или 75 дБм. Шумы в канале способны привести к высокому уровню ошибок передачи пакетов и нарушить беспроводную передачу, что снизит производительность сети или сделает сетевое подключение нестабильным.

Для каналов 5 ГГц (802.11a/n/ac) качество радиочастотного сигнала имеет следующую цветовую маркировку:

- Голубой: Указывает на то, что на канале обнаруживаются точки доступа (AP) и/или станции (ST).
- Темно-синий: Указывает на то, что на канале обнаруживаются межканальные помехи или станции, передающие сигналы зондирования.
- Красный: Указывает на то, что на канале обнаружены шумы.

Развертывание измерителя радиочастотного сигнала

По умолчанию панель измерителя радиочастотного сигнала свернута и показывает только сводку радиочастотных данных для каждого канала. Верхнюю или нижнюю часть измерителя радиочастотного сигнала можно разворачивать по отдельности, щелкая кнопкой мыши на (Развернуть) в правом верхнем углу каждой секции измерителя. На развернутом измерителе радиочастотного сигнала с помощью отдельных графиков отображается мощность сигнала, уровень шумов, отношение сигнал/шум и оценка помех для каждого канала.

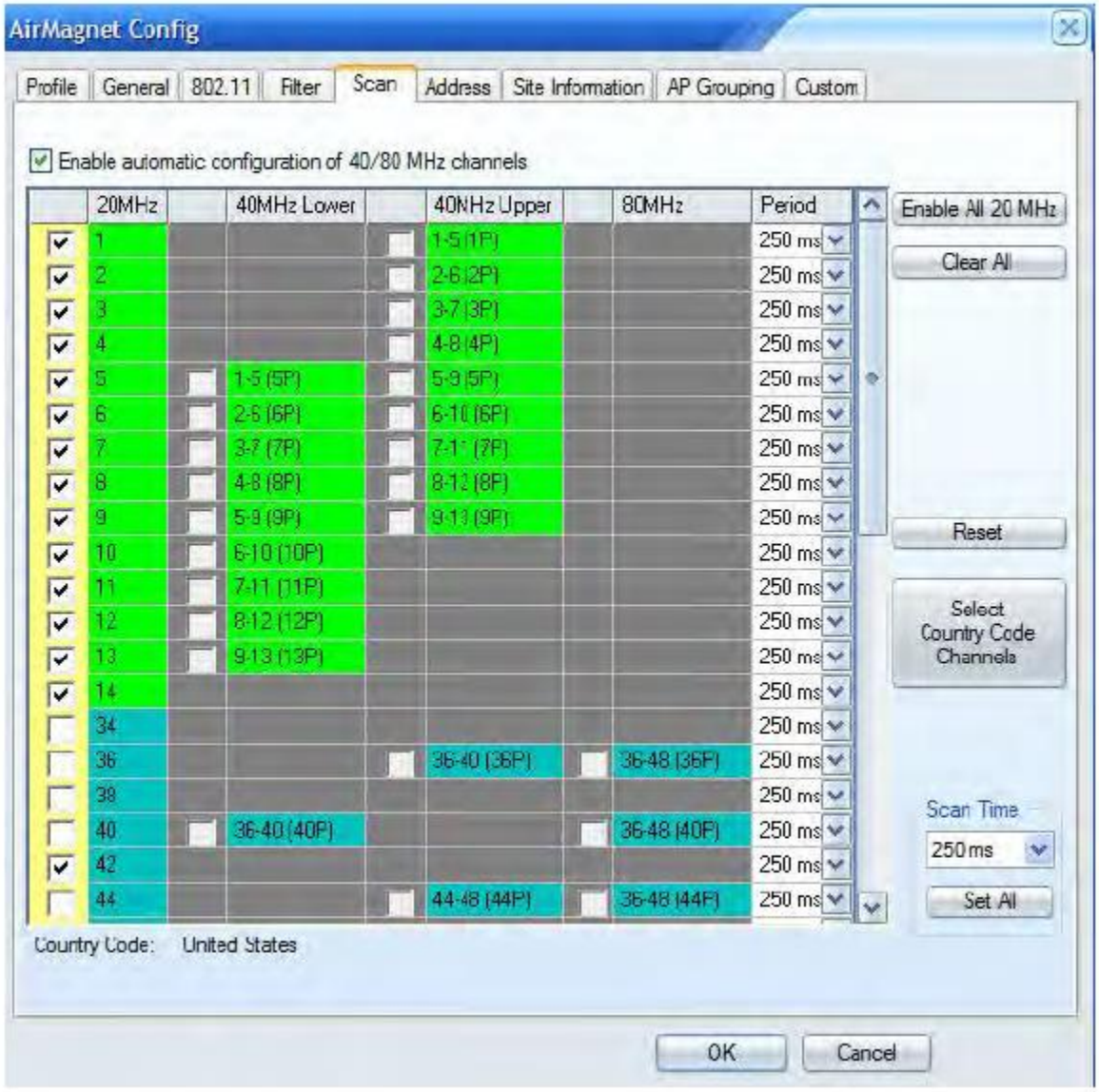
Чтобы восстановить исходное состояние измерителя радиочастотных сигналов, щелкните кнопкой мыши на (Свернуть) в правом верхнем углу развернутого экрана измерителя сигналов.

Подсказки:

- График оценки помех позволяет быстро просмотреть помехи, обнаруживаемые на каждом канале в настоящее время. Для более подробного просмотра щелкните кнопкой мыши на интересующем вас канале, что приведет к открытию страницы Interference (Помехи) для выбранного канала.
- Список сканирования каналов можно настроить, удалив неиспользуемые каналы и изменив частоту сканирования в диалоговом окне AirMagnet Configuration > Scan (Настройка конфигурации AirMagnet > Сканирование). Это позволит приложению AirMagnet WiFi Analyzer сосредоточиться на захвате

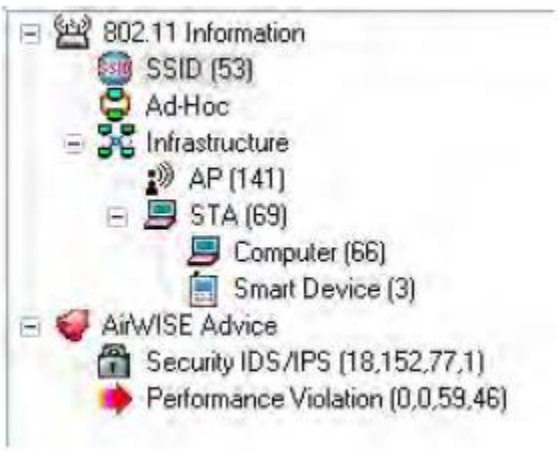
трафика на известных активных каналах, продолжая отслеживать наличие неавторизованных точек доступа и станций на этих неназначенных каналах.

- Двойной щелчок кнопкой мыши на канале в измерителе сигнала позволит напрямую открыть экран Channel (Канал), на котором можно провести целенаправленный анализ данных на этом канале.



Data Summary (Сводка данных)

Под измерителем радиочастотного сигнала находится сводка сетевых данных. Он представляет собой краткое изложение некоторой ключевой сетевой информации:

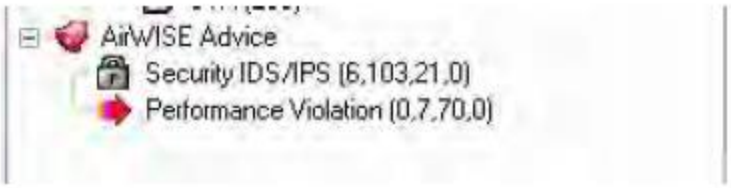


802.11 Information (Информация о 802.11)

Здесь сведены все сетевые компоненты или устройства, обнаруженные на беспроводной сети, и показано общее количество компонентов или устройств в каждой категории. Обратите внимание, что подсчет станций (STA) ведется отдельно для компьютеров (Computer) и интеллектуальных устройств (Smart Device).

AirWISE Advice (Советы AirWISE)

Здесь приводятся все тревоги, обнаруженные в вашей сети WLAN. Они делятся на две группы: безопасность и производительность. Для каждой категории имеется четыре набора цифр, представляющих разные уровни серьезности. Цифры слева направо представляют количество сигналов тревоги, которые являются критическими (Critical), срочными (Urgent), предупреждающими (Warning) или информационными (Informational).



Frame Count (Счетчик кадров)

В нижнем левом углу экрана Start находится таблица всех кадров, захваченных приложением AirMagnet WiFi Analyzer в вашей беспроводной сети.

Кадры делятся на следующие группы:

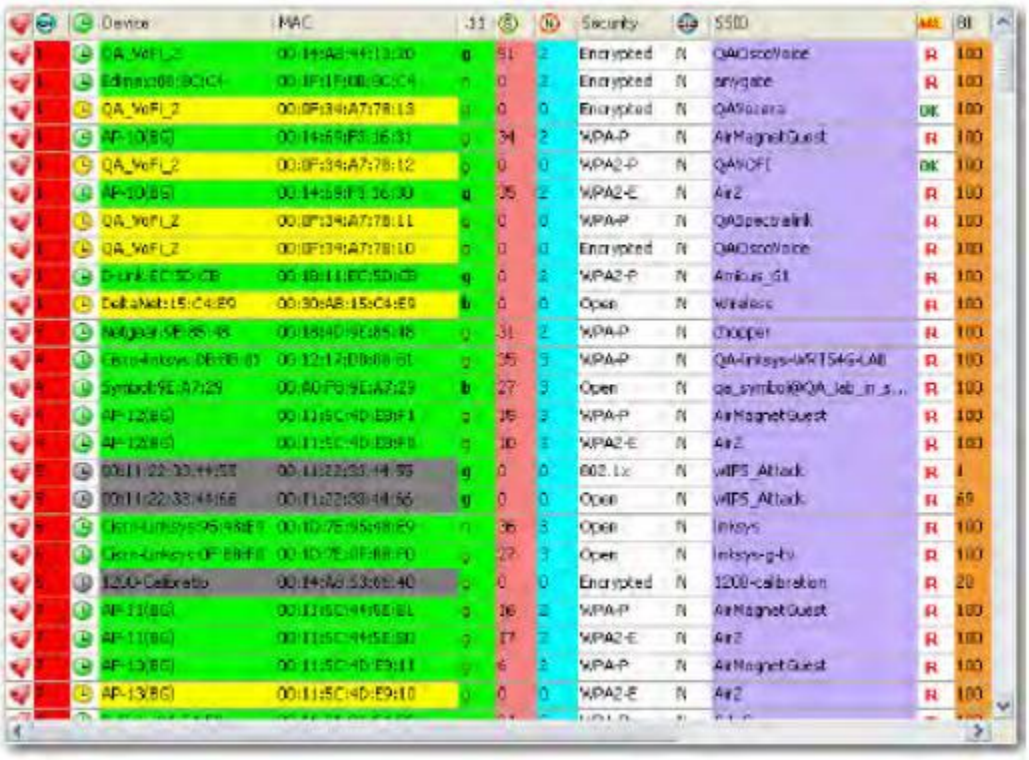
- Broadcast (Широковещательная передача): Широковещательная передача - это термин, используемый для описания связи, при которой данные передаются из одной точки на все другие точки. Другими словами, имеется только один отправитель, но информация отправляется всем подключенным получателям.
- Multicast (Многоадресная рассылка): Многоадресная рассылка - это схема связи, при которой исходный узел одновременно отправляет сообщение группе узлов назначения.
- Unicast (Одноадресная передача): Одноадресная передача - это термин, используемый для описания связи, при которой данные отправляются из одной точки в другую. Имеется только один отправитель и один получатель.
- CRC: Cyclic Redundancy Check (Циклический избыточный код) используется для проверки информации о пакетах и снижения вероятности возникновения ошибок.

Совет: Для отображения этой части экрана необходимо выбрать опцию Show Frame Statistics (Показать статистику кадров) в диалоговом окне AirMagnet Configuration > General (Настройка конфигурации AirMagnet > Общее).

Примечание: В поле Total Frames (Всего кадров) отображается общее количество кадров, обнаруженных в сети на данный момент. Поле справа позволяет увидеть, сколько (в процентах) каждый тип кадра составляет от общего количества кадров. Просто щелкните кнопкой мыши на направленной вниз стрелке и выберите в разворачивающемся меню тип кадра, который хотите посмотреть.

Device Data (Данные устройства)

Под панелью инструментов находятся такие вкладки, как Dashboard (Панель мониторинга), All Devices (Все устройства), AP (Точка доступа), STA (Станция) и Ad-hoc (Станция Ad-hoc). В верхнем правом углу экрана Start находится панель Device Data (Данные устройства), на которой собраны данные обо всех беспроводных устройствах, обнаруженных на сети WLAN.



Dashboard (Панель мониторинга)

Экран Dashboard (Панель мониторинга) включает шесть статистических диаграмм или таблиц. Для их добавления или удаления выбирайте из списка доступных диаграмм/таблиц в текущем списке Dashboard List. (Обратитесь к разделу «WiFi Dashboard (Панель мониторинга WiFi)»).

All Devices (Все устройства)

Устройства разделены на три категории, как указано в сворачивающихся секциях: точки доступа AP, станции Ad-Hoc и станции STA. Чтобы отобразить определенную категорию устройств, нажмите кнопку «-» в полях, которые вы хотите свернуть (например, для просмотра только станций сверните разделы AP и Ad-Hoc). Таблица содержит 49 полей данных, включая Channel (Канал), Device/MAC Address (Устройство/MAC-адрес), Display 802.11 (Показать 802.11), Signal Strength (Мощность сигнала), Noise Level (Уровень шумов), Signal-to-Noise Ratio (Отношение сигнал-шум), Security Mechanisms (Механизмы безопасности), TKIP и MIC, Bridge Mode (Режим моста), SSID, ACL Status (Статус ACL), Rogue in Network (Нарушитель в сети), Beacon Interval (Интервал сигнала маяка), Number of Stations (Количество станций), Preamble (Преамбула), PCF/DCF, Latitude (Широта), Longitude (Долгота), Altitude (Высота над уровнем моря), Distance (Расстояние), Tx Channel Width (Ширина канала передачи), Rx Channel Width (Ширина канала приема), SGI, First Seen Time (Время первого посещения) и Last Updated Time (Время последнего обновления).

Для сортировки данных по любой категории просто щелкните кнопкой мыши на заголовке соответствующего столбца, например SSID. Чтобы просмотреть все данные, содержащиеся в таблице, используйте полосу прокрутки внизу таблицы. Также можно настроить количество отображаемых столбцов данных.

Примечание: «n» в столбце .11 обозначает устройство 802.11n. Чтобы приложение AirMagnet WiFi Analyzer могло обнаруживать устройства 802.11n в сети, потребуется адаптер беспроводной сети 802.11n.

Для добавления/удаления отображаемых столбцов:

1. Щелкните правой кнопкой мыши в любом месте поля отображения данных и выберите в меню Set Display Columns (Установить отображаемые столбцы). Появится диалоговое окно Field Chooser (Выбор поля).

2. Перетащите заголовки столбцов из диалогового окна в столбцы таблицы. Перемещенный заголовок будет добавлен на страницу Start.
3. Для удаления заголовка из таблицы выполните шаг 2 в обратном порядке.

Совет: Двойной щелчок кнопкой мыши на поле в столбце тревог активирует экран AirWISE, на котором отображаются все сигналы тревоги, обнаруженные для этого устройства; двойной щелчок кнопкой мыши в любом другом столбце приведет прямо на экран Infrastructure (Инфраструктура).

Элемент	Описание
Type (Тип)	Отображается категория устройства, которая может быть одной из следующих: • AP (точка доступа) • STA (станция) • Ad-Hoc (станция ad-hoc)
Alarms (Тревоги)	Отображаются сигналы тревоги, связанные с устройством. Если устройство активировало сигналы тревоги, в этом столбце появляется значок тревоги (колокольчик).
Channel (Канал)	Все обнаруженные в сети WLAN доступные каналы: • Красный = на канале обнаружены сигналы тревоги. • Желтый = на канале не обнаружено никаких сигналов тревоги.
Active Time for Device (Активное время устройства)	Отображается текущее состояние устройства. Для отображения продолжительности активности устройства иконка имеет цветовую кодировку: • Зеленый = устройство было активно в течение последних 5 секунд. • Желтый = неактивно в течение последних 5 - 60 секунд. • Красный = неактивно в течение 60 - 300 секунд. • Серый = неактивно более 300 секунд.
AP Group (Группа точек доступа)	Если настроена функция группирования точек доступа (AP Grouping), отображаются имена групп точек доступа. Дополнительная информация приводится в разделе «Настройка группирования точек доступа».
Device (Устройство)	Отображается имя устройства. Часто в качестве имени по умолчанию используется MAC-адрес устройства. Для отображения состояния активности устройства это поле (и поле MAC Address (MAC-адрес) ниже) имеет цветовую маркировку: • Зеленый = устройство было активно в течение последних 5 секунд. • Желтый = устройство было неактивно в течение последних 5 - 60 секунд. • Красный = устройство было неактивно в течение последних 60 - 300 секунд. • Серый = устройство неактивно более 300 секунд.
MAC Address (MAC-адрес)	Отображается MAC-адрес устройства. В этом поле используется та же цветовая кодировка, что и в поле Device (Устройство) (смотрите выше).
.11 (802.11)	Тип среды 802.11, то есть 802.11b или 802.11g, которую использует устройство. • Зеленый = 802.11b • Оранжевый = 802.11g • Синий = 802.11a • Зеленый/синий = 2,4 ГГц 802.11n / 5 ГГц 802.11n • Лиловый = 5 ГГц 802.11ac
Signal (Сигнал)	Отображается уровень сигнала в % или дБм.
Noise (Шум)	Отображается уровень шума в % или дБм.
Signal-to-Noise Ratio (Отношение сигнал-шум)	Отображается отношение сигнал-шум, измеренное в % или дБм.
Interference Score (Оценка помех)	Отображается оценка помех канала.
Security Mechanisms (Механизмы безопасности)	Отображает механизмы безопасности, используемые на устройстве: • WPA-P = WPA-Personal. • WPA-E = WPA-Enterprise. • WPA2-P = WPA2-Personal. • WPA2-E = WPA2-Enterprise.

	• VPN = PPTP, IPsec, Secure Shell и так далее. • Open = нет механизма безопасности. • Encrypted = пакеты зашифрованы, но конкретный механизм шифрования неизвестен. • ? = механизм безопасности неизвестен. Для устройств, использующих несколько идентификаторов SSID, будут отображаться настройки безопасности для каждого из них, разделенные запятыми.
TKIP/MIC	Отображаются настройки безопасности TKIP/MIC: • Y = Включено. • N = Отключено. • U = Неизвестно. Для устройств, использующих несколько идентификаторов SSID, будут отображаться настройки безопасности для каждого из них, разделенные запятыми.
Bridge Mode (Режим моста)	Y = Используется режим моста. N = Режим моста не используется.
SSID	Отображается идентификатор SSID устройства.
ACL Status (Статус ACL)	Отображается статус ACL устройства.
	Примечание: При первом запуске приложения AirMagnet WiFi Analyzer после установки все обнаруженные устройства отображаются как U (Неизвестно). Необходимо изменить статус ACL (Список контроля доступа) всех устройств одно за другим. Для этого щелкните на устройстве правой кнопкой мыши и выберите Rogue Device, если это неавторизованное устройство, или Valid Device (Легитимное устройство), а затем, если это известное действительное устройство в сети, выберите определенную группу ACL из подменю. Все легитимные устройства отмечены OK. После того, как отмечен статус ACL устройства, оно будет отображаться на экране Start с таким же статусом ACL при следующем запуске приложения, если будет обнаружено то же устройство. Однако если все устройства отмечены как R (неавторизованные), то после запуска приложения после предыдущего выхода из него, все устройства будут отображаться как U (Неизвестно).
Rogue in Network (Нарушитель в сети)	Отображает неавторизованные устройства, отслеживаемые в корпоративной сети.
BI	Отображает Beacon Interval (Сигнальный интервал) (в миллисекундах).
Associated AP (Связанная точка доступа)	Отображает имя точки доступа, с которой связано устройство.
#STA	Отображает количество связанных станций.
Preamble (Преамбула)	Отображает значение преамбулы, которое может быть одним из следующих: • Long (Длинная). • Short (Короткая).
PCF/DCF	Показывает, используется ли функция координации точек (Point Coordination Function – PCF) или функция распределенной координации (Distributed Coordination Function – DCF).
Latitude (Широта)	Показывает широту устройства (только GPS).
Longitude (Долгота)	Показывает долготу устройства (только GPS).
Altitude (Высота над уровнем моря)	Показывает высоту устройства над уровнем моря (только GPS).
Distance (Расстояние)	Показывает расстояние до устройства (только GPS).
First (Первый)	Показывает время получения первого пакета.
Last (Последний)	Показывает время получения последнего пакета.
Cell Power (Мощность соты)	Показывает уровень мощности в дБм, на котором точка доступа осуществляет передачу.
Примечание:	Следующее применимо только к просмотру по 802.11n.
Tx Ch Width (Ширина канала передачи)	Отображает поддерживаемую ширину канала передачи (Tx).

Rx Ch Width (Ширина канала приема)	Задает ширину канала, которую можно использовать для передачи к точке доступа (AP) или станции (STA).
PCO	Показывает состояние PCO, которое может быть одним из следующих: • PCO активна в BSS. • PCO неактивна.
Greenfield Supported (Поддерживается Greenfield)	Показывает, поддерживается ли передача Greenfield; индикация может быть одной из следующих: • Y = Да. • N = Нет.
SGI	(Short Guard Interval/Короткий защитный интервал) Отображает короткий защитный интервал для 20 МГц и 40 МГц.
2nd Channel (2-й канал)	(Secondary Channel Offset/Смещение вторичного канала) Указывает смещение вторичного канала относительно первичного канала.
HT Protection (Защита HT)	Обозначает HT-защиту BSS, исходя из которой определяются требования защиты передачи в режиме HT (высокая пропускная способность).
Non-Greenfiels STA Present (Присутствует станция, не поддерживающая Greenfield)	Указывает, присутствуют ли станции, не поддерживающие Greenfield; может быть указано следующее: • N = Все станции совместимы с Greenfield. • Y = Одна или несколько подключенных HT-станций не поддерживают Greenfield.
Non-HT OBSS	(Присутствует станция OBSS Non-HT) • Y = Использовать защиту из-за OBSS. • N = Нет защиты из-за OBSS.
40 MHz Intolerant (Нетерпимость к 40 МГц)	Для точки доступа данный параметр указывает, должны ли BSS (Набор базовых служб) в пределах радиуса действия запрещать передачу по каналам 40 МГц; для станции указывает связанную с ней точку доступа, для которой в BSS требуется запретить все передачи 40 МГц.
RIFS Mode (Режим RIFS)	Отображает разрешение или запрещение режима RIFS (Reduced Interframe Space – Сниженное межкадровое пространство) для устройств 802.11n.
Tx STBC	(Поддерживается Tx STBC (передача с пространственно-временным блочным кодом)) Показывает, поддерживается ли Tx STBC; индикация может быть следующей: • Y = Поддерживается. • N = Не поддерживается.
Rx STBC	(Поддерживается Rx STBC (прием с пространственно-временным блочным кодом)) Показывает, поддерживается ли Rx STBC; индикация может быть следующей: • 0 = Не поддерживается. • 1 = Один поток. • 2 = Один и два потока. • 3 = Один, два и три потока.
LDPC	Отображает возможность кодирования LDPC (код с низкой плотностью проверок на четность), возможен любой из следующих вариантов: • Y = Да. • N = Нет.
SM Power Save (Энергосбережение SM)	Отображает режим энергосбережения SM.
Dual Beacon (Двойной сигнал маяка)	Показывает, используется ли двойной сигнал маяка: • Y = Точкой доступа передается вторичный сигнал маяка. • N = Вторичный сигнал маяка не используется.
Dual CTS Protection (Двойная защита CTS)	Показывает, требуется ли двойная защита CTS: • Y = Требуется. • N = Не требуется.
L-SIG TxOP Full Support (Полная поддержка L-SIG TxOP)	Показывает, поддерживается ли L-SIG TxOP: • Y = Все станции HT поддерживают защиту LSIG TxOP. • N = Одна или несколько станций HT не поддерживает защиту LSIG TxOP.
WAPI	WAPI (Инфраструктура аутентификации и конфиденциальности WLAN) - это китайский национальный стандарт для беспроводных локальных сетей (GB 15629.11-2003).

AP (Точка доступа)

Экран AP (Точка доступа) включает шесть статистических диаграмм или таблиц. Для добавления или удаления диаграмм/таблиц можно сделать выбор в списке доступных диаграмм и таблиц в текущем списке Dashboard List. (Обратитесь к разделу «Панель мониторинга WiFi»).

STA (Станция)

Экран STA (Станция) включает шесть статистических диаграмм или таблиц. Для добавления или удаления диаграмм/таблиц можно сделать выбор в списке доступных диаграмм и таблиц в текущем списке Dashboard List. (Обратитесь к разделу «Панель мониторинга WiFi»).

Ad-Hoc

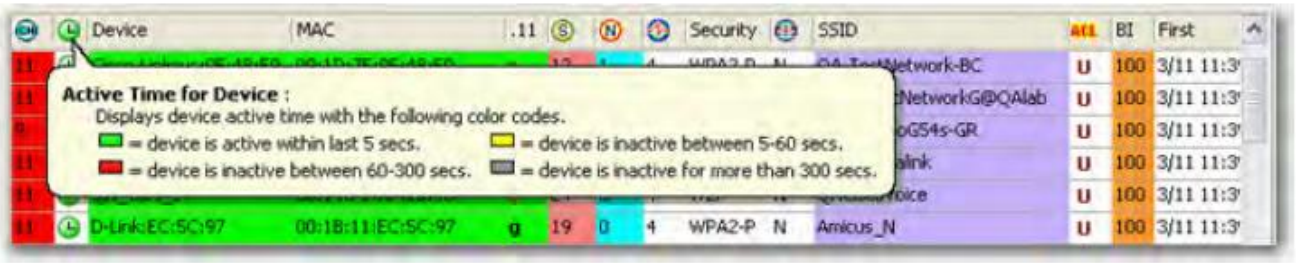
Экран Ad-Hoc (Станция Ad-Hoc) включает шесть статистических диаграмм или таблиц. Для добавления или удаления диаграмм/таблиц можно сделать выбор в списке доступных диаграмм и таблиц в текущем списке Dashboard List. (Обратитесь к разделу «Панель мониторинга WiFi»).

Live Network Data Pane (Панель сетевых данных в реальном времени)

В правом верхнем углу экрана Start находится панель сетевых данных в реальном времени, которая отображает исчерпывающие данные обо всех обнаруженных в сети WLAN беспроводных устройствах. Основная часть этого раздела представляет собой таблицу, в которой может отображаться более 30 типов данных об устройствах, по одному в каждом столбце таблицы.

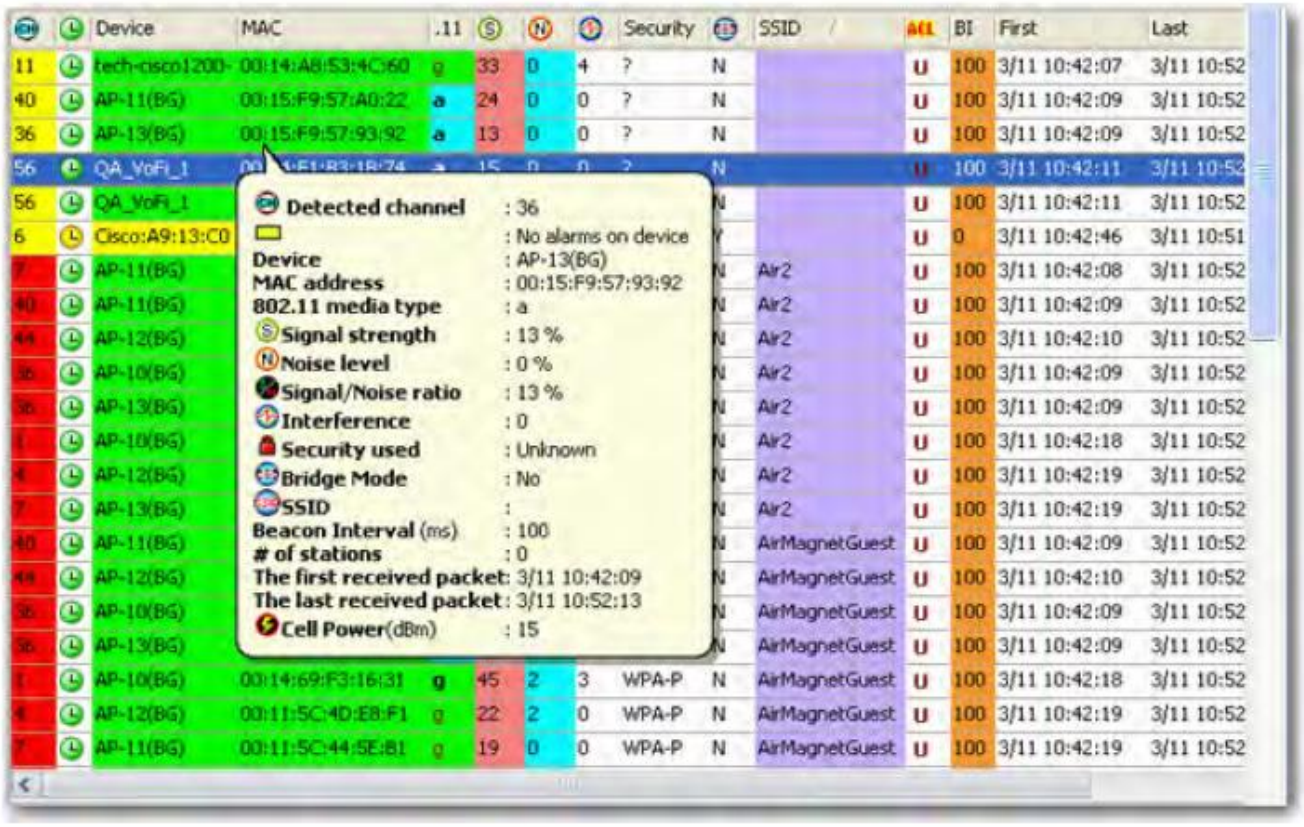
Подсказки:
Ниже приводится несколько советов, которые помогут эффективно использовать эту часть экрана Start.

- Устройства разделены на три категории: точки доступа AP, станции Ad-Hoc и станции STA. Чтобы отобразить или скрыть любую категорию устройств, щелкните кнопкой мыши на «+» или «-» в начале этого раздела.
- Чтобы понять значение данных в любом столбце, наведите курсор мыши на заголовок этого столбца. Во всплывающем экране подсказки будут предоставлено краткое описание этих данных.



Примечание: Чтобы воспользоваться этой функцией, необходимо включить функцию Bubble Help (Всплывающая справка).

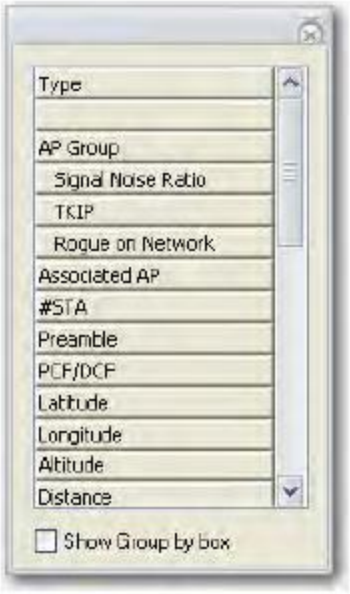
- Для просмотра различных данных об устройстве на экране наведите курсор мыши на любое поле в таблице. Для этого также необходимо включить всплывающую справку.



- Для сортировки данных по любой категории щелкните кнопкой мыши на заголовке соответствующего столбца, например SSID.
- Для просмотра данных, которые могут не помещаться на экран, используйте горизонтальную полосу прокрутки внизу таблицы.
- Выбирайте или изменяйте типы данных, которые будут отображаться в этой части экрана.

Чтобы выбрать данные для отображения на экране:

1. Щелкните правой кнопкой мыши в любом месте таблицы и выберите Set Display Columns (Установить столбцы на дисплее) во всплывающем меню. Появится диалоговое окно Field Chooser (Выбор поля).



2. Поля в диалоговом окне Field Chooser (Выбор поля) представляют собой потенциальные заголовки столбцов; перетащите их из диалогового окна в столбцы таблицы. Перемещенный заголовок будет добавлен на страницу Start.

3. Чтобы удалить столбец из таблицы, выполните шаг 2 в обратном порядке.
4. Чтобы отображать разные типы данных в порядке наложения, установите метку в поле Show group by box (Показывать группировку по полю).
5. По завершении закройте диалоговое окно.

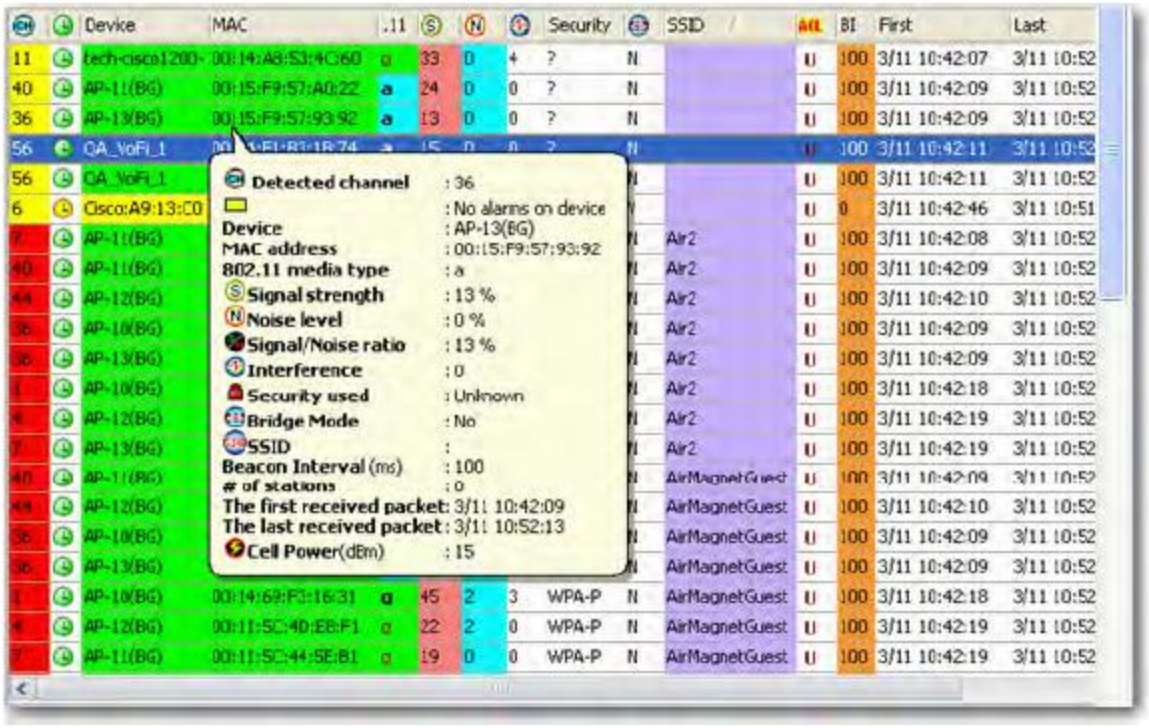
Поиск беспроводного устройства с экрана Start

Для быстрого получения доступа к инструменту поиска (Find Tool) для определенного устройства с экрана Start щелкните на нужном устройстве правой кнопкой мыши и выберите Find (Найти) во всплывающем меню. Это откроет Find Tool (Инструмент поиска) AirMagnet, который даст возможность физически найти устройство. Инструкции по использованию инструмента Find Tool приводятся в разделе «Обнаружение неавторизованных устройств».

Использование всплывающей справки

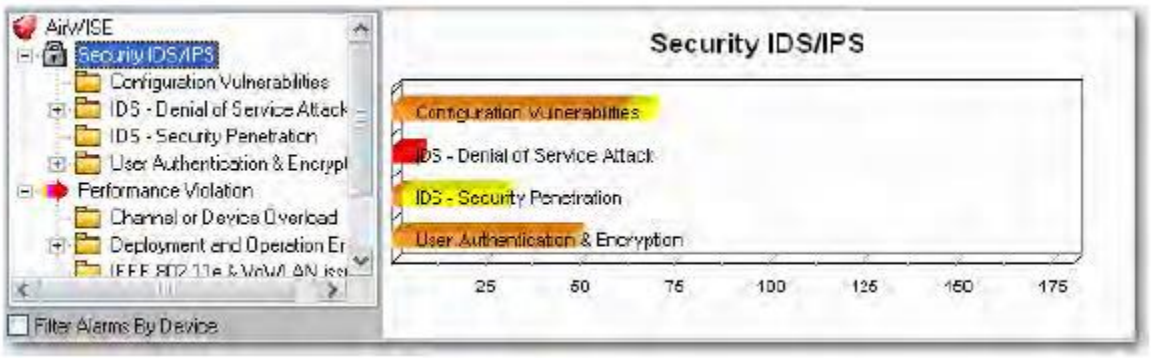
Кнопка  (Показать/скрыть всплывающую справку) позволяет включать или отключать всплывающую справку, которая представляет собой контекстно-зависимый экран подсказки, доступный только для разделов Signal Meter (Измеритель сигнала), 802.11 Information and AirWISE Advice (Информация 802.11 и советы AirWISE) и Device Data (Данные устройства) на экране Start. То есть в тех частях экрана, где текстовые надписи невозможно реализовать из-за нехватки места, полезная информация предоставляется во всплывающей справке.

Чтобы воспользоваться всплывающей справкой, щелкните кнопкой мыши на  и затем наведите курсор мыши на объект в любом из этих разделов.



AirWISE Details (Подробности AirWISE)

Под разделом данных устройства находится раздел AirWISE, в котором представлена подробная информация обо всех сработавших сетевых тревогах. Эта часть экрана состоит из двух частей (левой и правой). Слева находятся сигналы тревоги, касающиеся безопасности и производительности, каждая из которых далее разбита на различные подкатегории. Справа же находится гистограмма, на которой отображается количество сигналов тревоги в выбранной категории.



Примечание: В нижнем левом углу этого раздела находится поле выбора Filter Alarms by Device (Фильтровать сигналы тревоги по устройствам). Обычно панель AirWISE отображает информацию обо всех тревогах, инициированных всеми устройствами (то есть точками доступа, станциями STA или станциями Ad Hoc), отображаемыми на экране. Однако если в поле Filter Alarms by Device (Фильтровать сигналы тревоги по устройствам) стоит метка, в разделе панели AirWISE будет отображаться только информация об устройстве, будь то точка доступа, станция или станция Ad Hoc, которая выбрана выше на панели данных трафика в реальном времени.

Подсказки:

- Для отображения панели AirWISE необходимо выбрать опцию Show AirWISE в диалоговом окне Configuring General System Parameters (Настройка общих параметров системы).
- Чтобы скрыть панель AirWISE с экрана Start, щелкните на ней правой кнопкой мыши и выберите во всплывающем меню Hide AirWISE (Скрыть AirWISE).

Изменение рабочей частоты

Беспроводные устройства в беспроводной сети для передачи и приема пакетов могут использовать разные рабочие радиочастоты, в зависимости от используемого беспроводного сетевого протокола 802.11. Приложение AirMagnet WiFi Analyzer поддерживает все протоколы 802.11, то есть 802.11a/b/g/n/ac. Поскольку базирующиеся на разных стандартах 802.11 беспроводные устройства используют разные рабочие частоты, выбор или изменение рабочей частоты в приложении AirMagnet WiFi Analyzer заставляет его собирать пакеты, которые создаются только устройствами, использующими определенную рабочую частоту радиосвязи. Это позволяет сосредоточиться на сетевом трафике с участием беспроводных устройств, использующих определенный протокол 802.11.
В разворачивающемся меню Operating Frequency (Рабочая частота) перечислены все рабочие частоты, поддерживаемые беспроводной сетевой картой, которая в настоящее время используется в приложении AirMagnet WiFi Analyzer.

Изменение рабочей частоты похоже на физическую замену беспроводной сетевой карты. Приложение AirMagnet WiFi Analyzer удалит из буфера все захваченные пакеты, а затем начнет сбор данных, используя новую рабочую частоту. Любое изменение рабочей частоты отражается в других затрагиваемых частях пользовательского интерфейса. Если открыт любой экран, отличный от экрана Start, выбор другого частотного диапазона приведет к переходу прямо на экран Start.

Протоколы 802.11 и рабочие частоты

Протокол	Рабочая частота (ГГц)	Типовая пропускная способность (Мбит/с)	Максимальная скорость передачи данных (Мбит/с)	Рабочее расстояние в помещении (метров)	Рабочее расстояние вне помещения (метров)
802.11a	5,15 ~ 5,25 5,25 ~ 5,35	23	54	~ 27	~ 90

	5,745 ~ 5,825				
802.11b	2,4 ~ 2,5	4	11	~ 31	~ 100
802.11g	2,4 ~ 2,5	19	54	~ 31	~ 100
802.11n	2,4 и / или 5	74	248	~ 63	~ 144
802.11ac	5	200 - 250	1 Гбит / с	~ 17	Нет данных

Режим FCC 4,9 ГГц

В качестве лицензированного частотного диапазона 4,9 ГГц обеспечивает рабочую среду без помех для широкополосной связи в области общественной безопасности. Он лучше всего подходит для фиксированных беспроводных приложений обеспечения связи точка-точка (P2P) и точка-многоточка (PMP). Существует ряд услуг, которые государственное учреждение или муниципальный орган может предоставить на базе магистральной сети передачи 4,9 ГГц. Обычно эти услуги и приложения способны заменять дорогостоящие арендуемые услуги, что для органа власти приводит к окупаемости инвестиций и долгосрочной экономии. В настоящее время приложение AirMagnet WiFi Analyzer является единственным программным обеспечением анализа WLAN, способным контролировать частотный диапазон 4,9 ГГц.

Примечание: Функция 4,9 ГГц работает только с адаптерами Ubiquiti SR4C 4,9 ГГц и TRENDnet TEW-501PC ag.

Изменение единиц измерения радиочастотного сигнала

По умолчанию мощность радиочастотного сигнала канала, уровень шумов и отношение сигнал-шум отображаются в процентах (%). Однако щелкнув на разворачивающемся меню %/dBm рядом с кнопкой типа среды, можно перейти на дБм.

При переключении между % и дБм обратите внимание на изменения, произошедшие в полях сигнала, шумов и отношения сигнал-шум в разделе Device Data (Данные устройства).

Распределение радиоканалов 802.11 a/b/g/n/ac по всему миру

Поскольку радиочастоты (каналы) и мощность излучения для стандартов 802.11 в различных частях мира определяются нормативными правилами, количество доступных каналов зависит от географического положения и выбранного частотного диапазона (2,4 ГГц или 5 ГГц).

Регион / Страна	2,4 ГГц	5 ГГц
Америка	1 ~ 11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 132, 136, 149, 153, 157, 161, 165
Большая часть Европы и Австралия	1 ~ 13	36, 40, 44, 48, 52, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Франция	10 ~ 14	36, 40 44, 48, 52, 56, 60, 64
Испания	10 ~ 11	36, 40 44, 48, 52, 56, 60, 64
Япония	1 ~ 14	36, 40, 44, 48, 52, 56, 60, 64
Тихоокеанский регион (Китай, Тайвань, Гонконг, Сингапур, Корея и т.д.)	1 ~ 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

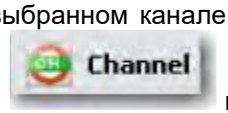
На экране Start отображается информация верхнего уровня о радиочастотной среде вашей беспроводной локальной сети. Это особенно полезно, если необходимо быстро понять, что происходит внутри или вокруг сети WLAN. Однако имейте в виду, что данные на этом экране являются динамическими и отображаются в реальном времени. По мере поступления новых данных старые данные стираются. Именно по этой причине приложение AirMagnet WiFi Analyzer поставляется с функцией захвата в реальном времени, которая позволяет записывать (сохранять) данные для их последующего воспроизведения и анализа. Также данные можно экспортировать. Для получения дополнительной информации обратитесь к разделу «Сохранение захваченных данных».

Получение доступа к отчетам с данными

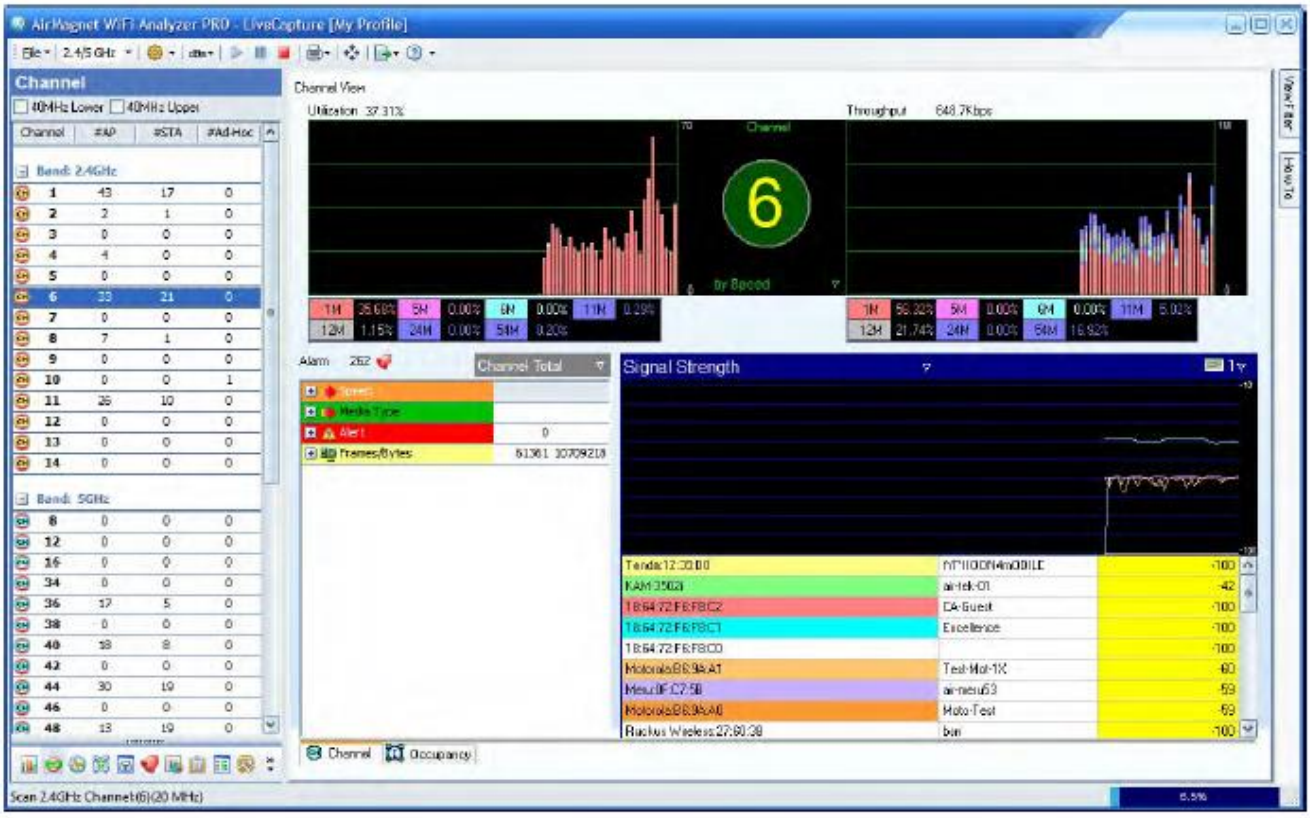
Встроенная функция AirMagnet Reporter автоматически преобразует все данные на экране в отчеты. Содержание отчетов зависит от экрана, что упрощает их просмотр, анализ, совместное использование и архивирование. Подробные инструкции по использованию функции Reporter можно найти на панели отчетов (Report).

Экран Channel (Канал)

Об экране Channel (Канал)

Экран Channel (Канал) позволяет сосредоточиться на проблемах, связанных с различными беспроводными устройствами на выбранном канале. Для перехода на экран Channel (Канал) в любой момент щелкните кнопкой мыши на 

на панели навигации.



Использование (Utilization) и пропускная способность (Throughput) канала

В верхней части экрана расположены два измерителя сигнала: один для использования канала (Utilization), а другой для пропускной способности канала (Throughput). Как показывает практика, использование в 60% или пропускная способность в 6 Мбит/с - это реалистичный верхний предел для сети 802.11b. Постоянное высокое использование канала с большей частью трафика в 11 Мбит/с и низкой частотой ошибок пакетов может указывать на то, что сеть 802.11b, возможно, не имеет достаточной пропускной способности для удовлетворения потребностей всех своих пользователей. Одно из возможных решений - уменьшить размер соты и добавить точки доступа в стратегически важных местах.

Панель выбора канала

В левой части экрана находится панель выбора канала (Channel Selection). Список каналов основан на том, какой частотный диапазон (2,4 ГГц, 5 ГГц или оба) выбран на панели инструментов.

Каналы сканируются в соответствии с настройками Channel (Канал) на вкладке Config > Scan (Конфигурация > Сканирование). Обратитесь к разделу «Настройка сканирования каналов». Эти настройки могут быть временно отменены с помощью описанной ниже опции. Настройки Channel (Канал) будут восстановлены после того, как вы покинете экран канала.

На панели выбора канала имеются четыре столбца: Channel, #AP, #STA и #Ad-Hoc. В этих столбцах отображаются номера каналов и количество точек доступа, станций и устройств Ad-Hoc на каждом канале. При сканировании номер соответствующего канала отображается в строке состояния в нижней части пользовательского интерфейса.
Если канал включает в себя верхние или нижние 40 МГц, строка состояния будет включать эту информацию по мере сканирования канала.
Для канала, который включает в себя верхние или нижние 40 МГц, сканирование каналов может быть дополнительно задано с помощью полей для установки меток в верхней части панели выбора канала. Эти поля позволяют сосредоточиться на сканировании пакетов HT (Высокая пропускная способность), как описано в следующих пунктах:

- Lower 40 MHz (Нижний 40 МГц) – Если выбрано, отображается нижний канал 40 МГц. Пакеты сканируются в нижнем канале 40 МГц и в канале 20 МГц.
- Upper 40 MHz (Верхний 40 МГц) – Если выбрано, отображается верхний канал 40 МГц. Пакеты сканируются в верхнем канале 40 МГц и в канале 20 МГц.
- 80 MHz (80 МГц) – При использовании поддерживаемого адаптера 802.11ac можно сканировать пакеты в канале 80 МГц.

Щелкните кнопкой мыши на списке каналов на панели выбора канала, и на экране канала справа от панели выбора канала отобразится подробная информация о нем.
Для переключения с одного канала на другой щелкайте кнопкой мыши в списке каналов на панели выбора. После выбора канала приложение AirMagnet WiFi Analyzer фиксируется на этом канале до тех пор, пока не будет выбран другой канал. Выбранный канал обозначается числом внутри круга в центре верхней части экрана.

В нижней части графика отображается скорость, с которой по выбранному каналу передаются пакеты. Эти поля имеют цветовую кодировку и соответствуют приведенным выше графикам использования. Если весь график красный, практически все пакеты в сети передаются со скоростью 1 Мбит/с.

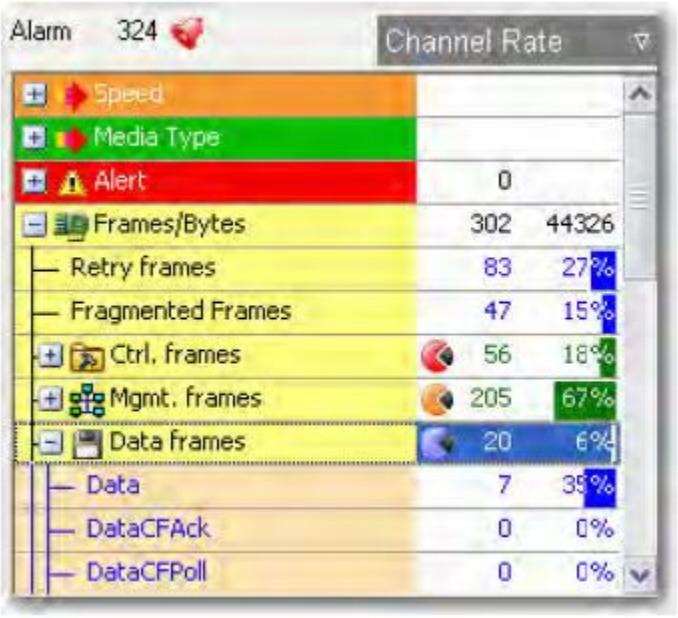
Скорость связи (Link Speed) и тип среды (Media Type)

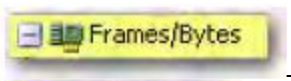
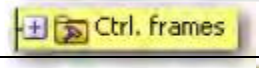
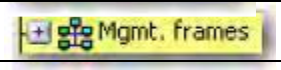
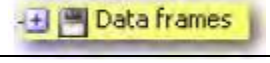
Если в качестве типа среды используется 802.11g, a/g или a/b/g/n/ac, под номером канала появляется фильтр, позволяющий переключать отображение данных между скоростью связи и типом среды. И скорость связи, и тип среды имеют цветовую кодировку. При выборе по скорости в полях под графиками отображаются различные скорости передачи данных; выбор по типу среды отображает среды передачи пакетов данных.

Сводка данных канала

Слева в середине экрана Channel (Канал) содержится различная важная информация о выбранном канале.
Вверху находится сводка сигналов тревоги для этого канала. Здесь отображается количество сработавших сигналов тревоги на канале. Щелчок кнопкой мыши на позволяет перейти на экран AirWISE с подробным объяснением сигналов тревоги и экспертными советами.
Под сводкой сигналов тревоги находится сводка радиочастотных данных для выбранного канала. Все данные отображаются в кадрах или байтах. Каждый тип данных представлен определенной иконкой. Щелкая кнопкой мыши на значке «плюс» или «минус» рядом с соответствующей иконкой можно просмотреть подробную информацию о любых из этих данных или скрыть их. Также можно отфильтровывать отображение данных по скорости канала (Channel Rate) или по количеству переданных

данных по каналу (Channel Total), используя опции разворачивающегося меню в правом верхнем углу панели сводки.



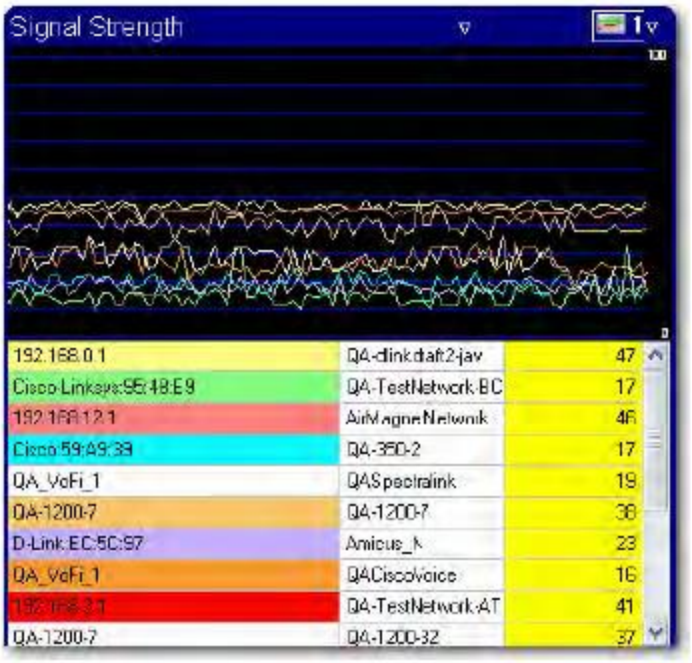
Кнопка	Описание
	Обобщает скорость связи канала.
	Обобщает типы сред, обнаруженных на канале.
	Перечисляет информацию о кодах ошибок кадров.
	Позволяет разделить счетчики кадров и байтов на повторно переданные кадры, фрагментированные кадры, управляющие кадры, кадры менеджмента, кадры данных, кадры ошибок CRC и т.д.
	Обобщает управляющие кадры/байты.
	Обобщает кадры/байты менеджмента.
	Обобщает кадры/байты данных.

Экран Channel (Канал) позволяет легко обнаруживать низкие скорости связи, чрезмерное количество повторных попыток и ошибки циклического избыточного кода (CRC).

График данных устройства

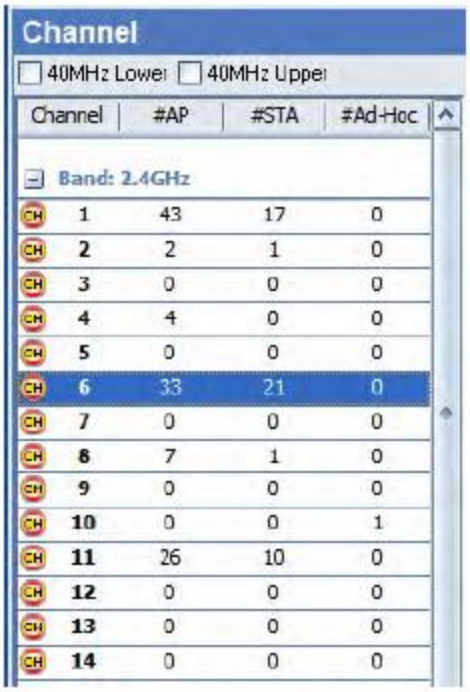
В этой части экрана Channel (Канал) отображаются различные типы сетевых данных в виде линейных диаграмм. В верхней части этого экрана находятся два фильтра. Тот, что слева, предоставляет до дюжины типов данных, которые можно выбрать для графика, а тот, что справа, позволяет выбрать количество одновременно отображаемых графиков (от 1 до 6).

На этом рисунке показаны отображаемые в нижней правой части экрана Channel (Канал) данные устройства на выбранном канале. Вверху расположены два фильтра. Расположенный слева Data Selector (Выбор данных) позволяет выбрать тип отображаемых данных, а расположенный справа Graph Options (Опции графика) позволяет выбрать отображение данных на отдельных миниатюрных экранах (до шести).
Таблица под графиком содержит информацию для выбранного типа графика. На графике по умолчанию (Signal Strength/мощность сигнала) отображаются все обнаруженные на канале устройства. Каждое устройство имеет уникальный цвет, соответствующий цвету на линейной диаграмме выше. Если какое-либо из устройств имеет справа нулевое значение, то оно вообще не будет отображаться на графике.



Варианты экрана Channel (Канал)

Экран Channel (Канал) представлен в двух вариантах: Channel (Канал) и Occupancy (Занятость). Первый используется для анализа радиочастотных условий на выбранном канале, тогда как второй предназначен для анализа состояния занятости канала или использования полосы частот. Для переключения между ними нажмите на вкладку Channel (Канал) и Occupancy (Занятость) внизу экрана.



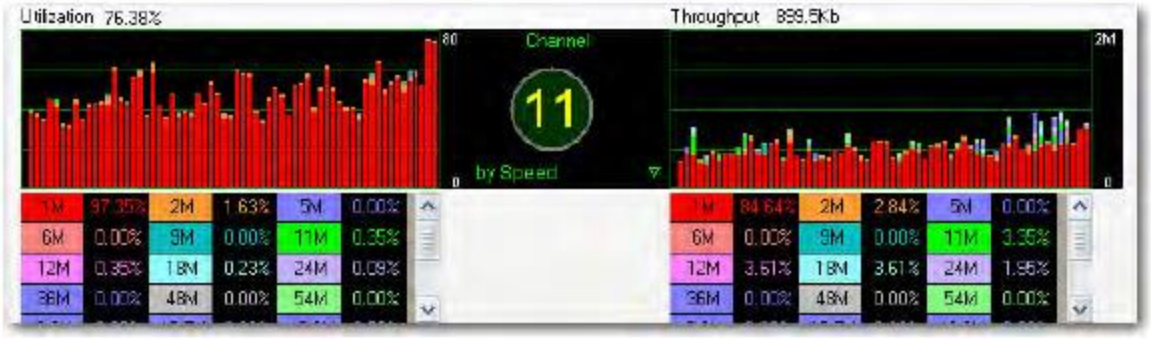
Анализ радиочастотных условий по каналам

По умолчанию при открытии экрана Channel (Канал) вкладка Channel (Канал) выбирается автоматически. Эта версия экрана Channel позволяет просматривать и детально анализировать огромное количество радиочастотных данных, захваченных на каждом канале беспроводной сети. Это не только обеспечивает подсчет устройств каждого типа на каждом канале, но также позволяет сосредоточиться на одном конкретном канале для более глубокого его анализа.

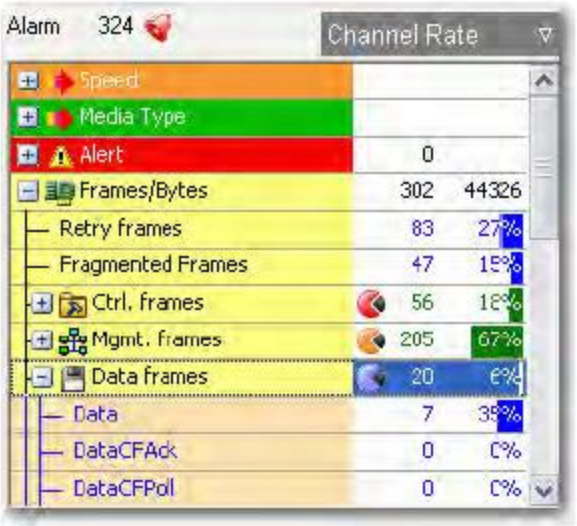
Экран включает следующие разделы:

- Количество устройств на каждом канале – В этой части экрана отображаются все доступные каналы по частотному диапазону (то есть 2,4 ГГц или 5 ГГц) и количество беспроводных устройств в каждой из трех категорий (то есть точки доступа AP, станции STA и устройства Ad-Hoc) на каждом канале.

- Использование (Utilization) и пропускная способность (Throughput) канала – В этой части экрана отображается статистика использования (слева) и пропускной способности (справа) выбранного канала в реальном времени. Число в середине экрана обозначает рассматриваемый в данный момент канал. Данные можно отображать по скорости (по умолчанию) или по частотному диапазону, щелкнув кнопкой мыши на направленной вниз стрелке и выбрав нужный вариант в разворачивающемся списке.

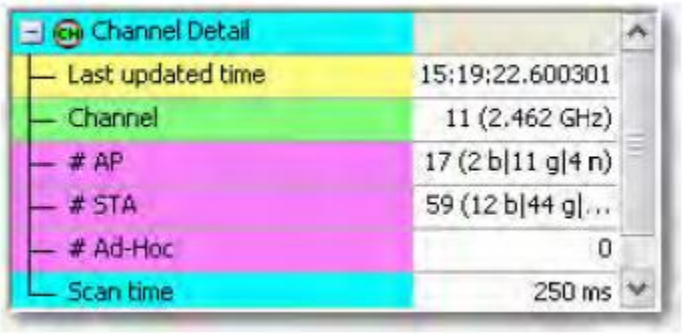


- Анализ радиочастотных данных канала – В этой части экрана представлен подробный анализ данных по четырем категориям (скорость, тип среды, тревоги и кадры/байты), каждую из которых затем можно разделить на подкатегории. Статистику можно просматривать либо по Channel Total (общему количеству переданных данных по каналу) (по умолчанию), либо по Channel rate (Скорость канала), щелкнув на направленной вниз стрелке в правом верхнем углу этой части экрана и выбрав любую из опций. Число в верхнем левом углу этой части экрана отображает общее количество тревог, обнаруженных на текущем канале.



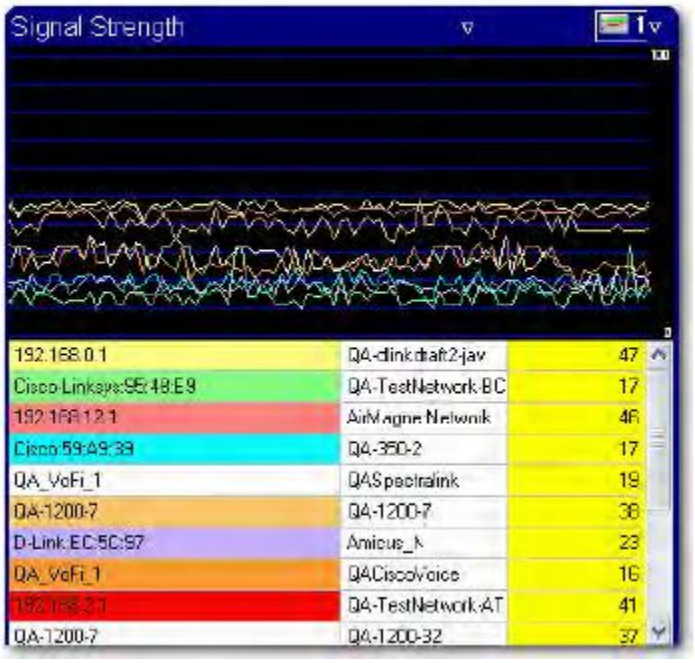
- Сведения о канале (Channel Detail) - В этой части экрана отображается основная статистика о текущем канале.

Примечание: Для отображения этой части экрана Channel (Канал) может потребоваться экран большего размера или увеличение разрешения текущего экрана.



- Графики данных – Эта часть экрана позволяет отображать различные типы сетевых данных в виде линейной диаграммы. Вверху этого экрана расположены два фильтра. Тот, что слева, предоставляет до дюжины типов данных, которые можно выбрать для отображения на графике, а тот, что справа, позволяет выбирать количество одновременно отображаемых графиков (от 1 до 6).

Примечание: Внизу этой части экрана отображается информация, относящаяся к тому типу данных, который выбран с помощью фильтра данных выше. График по умолчанию (Signal Strength/мощность сигнала) отображает устройства на канале; эти устройства отображаются на экране в виде графиков. Цвет каждого устройства соответствует цвету, которым на графике будут отображаться соответствующие линии. Если какое-либо из устройств имеет справа нулевое значение, график отображаться не будет.



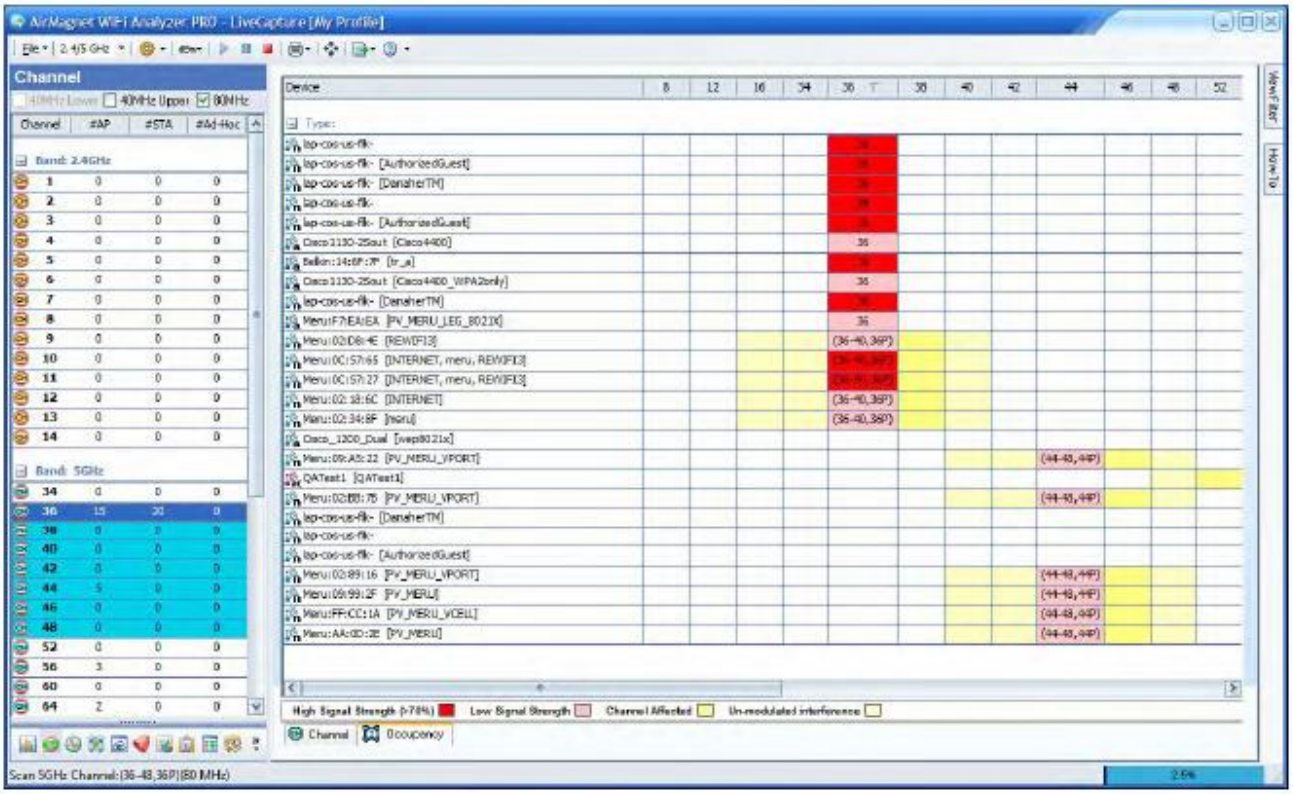
Анализ занятости канала по полосе частот

Экран занятости канала (Channel Occupancy) обеспечивает «вид с высоты птичьего полета» на использование радиочастотного спектра устройствами 802.11 в полосе частот 2,4 или 5 ГГц (в зависимости от выбранного канала). Здесь в режиме реального времени отображается состояние занятости (или использования) всех доступных каналов, что предоставляет пользователю простой и понятный способ узнать, какие каналы используются и какие каналы им следует выбрать, если они хотят получить более высокое качество сигнала (с меньшими помехами).

Для каждого устройства 802.11 на экране занятости канала (Channel Occupancy) отображается следующая информация:

- Имя устройства и тип среды передачи.
- «Центральный» канал (частота) устройства, определяемая положением красного квадрата.
- Уровень сигнала устройства, который отражает интенсивность красной окраски «ячейки центрального канала». Чем темнее красный цвет, тем выше уровень сигнала.

- Канал устройства, указанный в виде числового значения в центральной ячейке канала; для каналов 40 и 80 МГц указывается диапазон каналов, за которым следует первичный канал (P). Например (44-48, 44P) обозначает канал 40 МГц с основным на канале 44.
- Использование модулированного спектра устройства, как показано желтыми ячейками в его строке; и использование немодулированного спектра устройства, как показано светло-желтыми ячейками в соответствующей строке.



На приведенном выше примере экрана отображается следующая информация о первых пяти перечисленных устройствах:

- Они работают на канале 1 диапазона 2,4 ГГц.
- Пятое устройство имеет самый слабый сигнал из пяти.
- Все пять устройств вносят модулированные помехи на каналах 2 и 3.
- Все пять устройств создают (по крайней мере, некоторые) немодулированные помехи на каналах с 4 по 7.

Также можно просмотреть следующую информацию о 7-м и 8-м перечисленных устройствах:

- Эти устройства работают на частоте 40 МГц (нижний), канал 11.
- Модулированные помехи распространяются на две дополнительные ячейки по обе стороны от центральной частоты по сравнению с устройствами 20 МГц, описанными выше.
- Немодулированные помехи распространяются до канала 1.
- Центральная частота устройства сдвинута на 10 МГц (на что указывает тот факт, что центральный канал находится под столбцом канала 9 вместо 11).

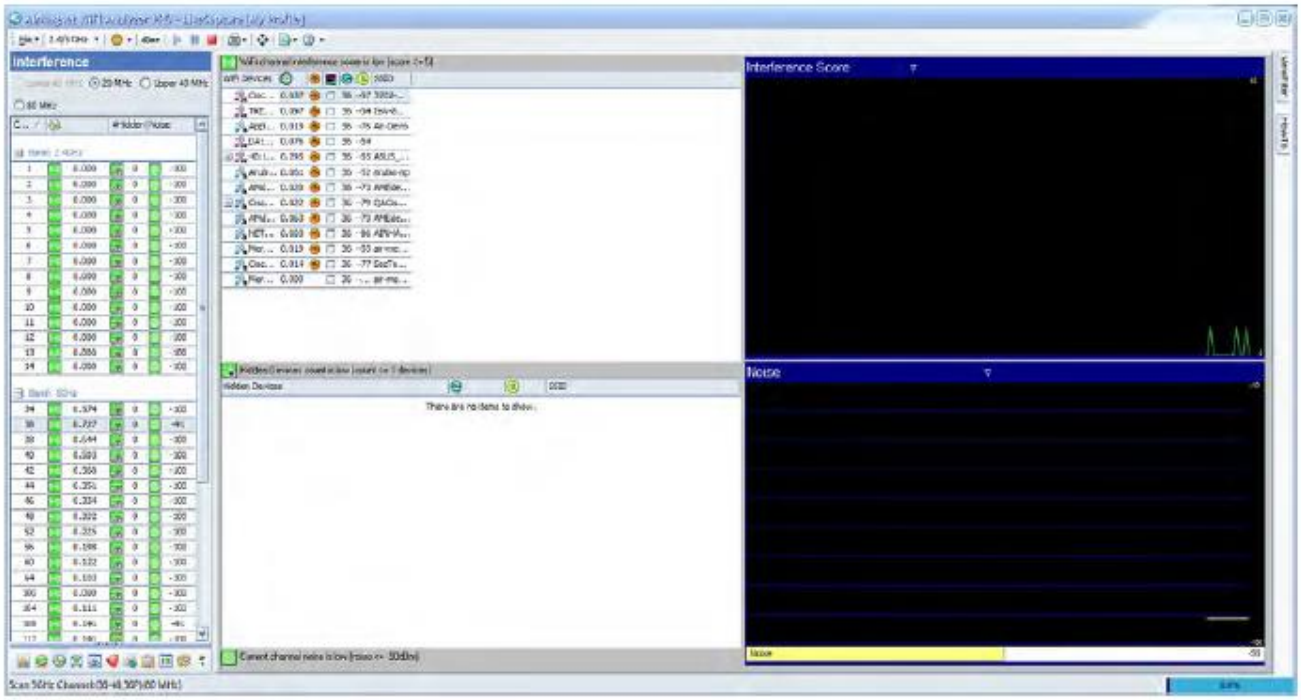
Примечание: Занятость каналов 2,4 ГГц и 5 ГГц отличается друг от друга тем, что каналы 5 ГГц разнесены на 20 МГц по сравнению с разнесением в 5 МГц для каналов 2,4 ГГц. Таким образом, устройства будут занимать меньше ячеек в режиме просмотра 5 ГГц, чем в режиме просмотра 2,4 ГГц.

Экран Interference (Помехи)

Об экране Interference (Помехи)

Экран Interference (Помехи) позволяет просматривать и анализировать помехи радиочастотного сигнала на заданном канале. Для перехода на экран помех щелкните кнопкой мыши на 

на панели навигации. Экран помех показан на следующем рисунке.



Экран Interference (Помехи) позволяет просматривать уровень помех сигнала, которые в настоящее время существуют на данном канале. Оценка помех для выбранного канала отображается в цифровом виде, а также в виде графика справа от списка устройств. Оценка помех отражает ту степень, с которой помехи влияют на производительность вашей сети. Чем выше значение, тем серьезнее воздействие.

Примечание: Оценка помех для канала полностью рассчитывается для стандартных устройств Wi-Fi. Каждое устройство, работающее на выбранном канале или на соседних каналах, будет создавать помехи на рассматриваемом канале. Отображаемая оценка помех суммирует помехи от этих устройств и показывает, какое воздействие помех в результате испытывает канал. Оценка помех для каждого отдельного канала может сильно различаться из-за разного количества устройств, работающих в соседних каналах.

Оценки помех

Оценка помех для канала полностью рассчитывается для стандартных устройств Wi-Fi. Каждое устройство, работающее на выбранном канале или на соседних каналах, будет создавать помехи на рассматриваемом канале. Отображаемая оценка суммирует помехи от этих устройств и показывает, какое воздействие помех в результате испытывает канал. Оценка помех для каждого отдельного канала может сильно различаться из-за разного количества устройств, работающих в соседних каналах.

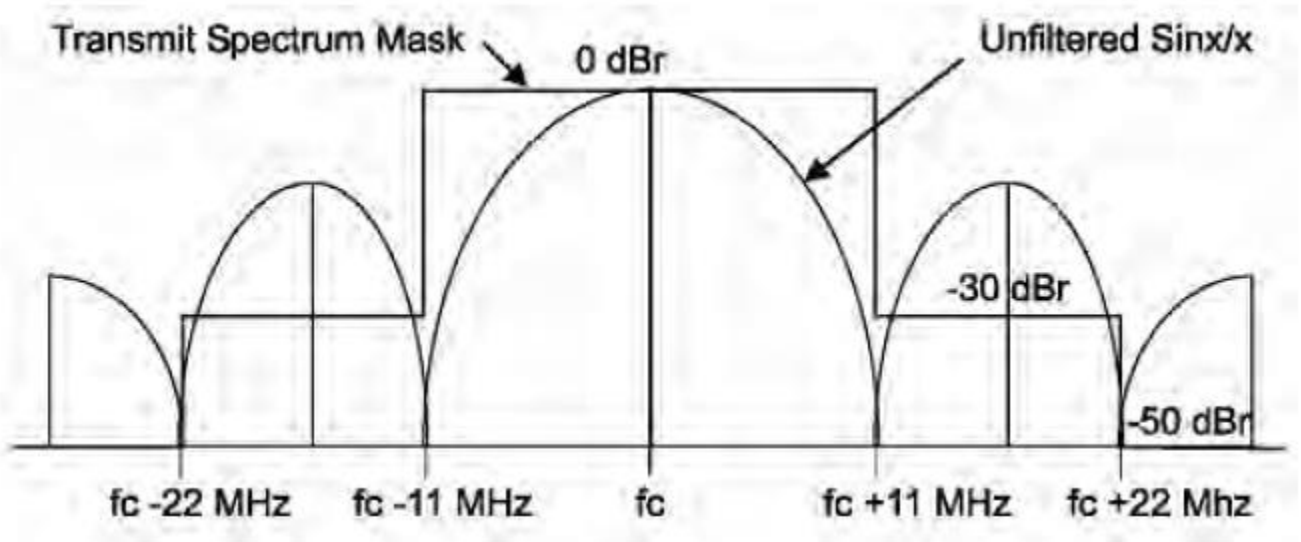
Если приложение AirMagnet WiFi Analyzer используется само по себе (не в сочетании с анализатором спектра), отображаемые помехи представляют собой сумму всех стандартных помех, создаваемых на выбранном канале устройствами 802.11 (точками доступа, устройствами Wi-Fi, беспроводными станциями и т.д.). Любая помеха, не связанная со стандартом 802.11, отображается как шум, который можно просмотреть, выбрав опцию Noise graph (График шумов) в правом нижнем углу экрана. Для определения источника шумов (то есть объектов или устройств, которые приводят к его появлению) можно приобрести

AirMagnet Spectrum Analyzer и объединить его с приложением AirMagnet WiFi Analyzer. Обратитесь к разделу «Интеграция анализатора спектра AirMagnet Spectrum Analyzer».

Расчеты помех

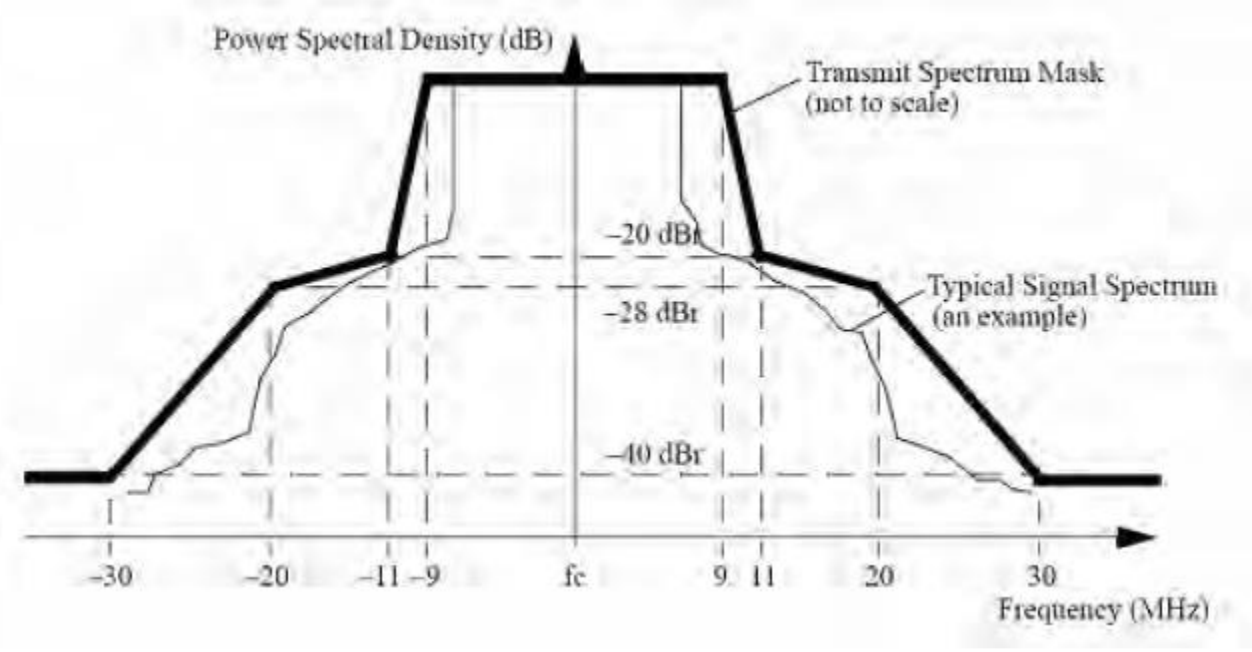
Стандарт 802.11 определяет требования к маске спектра радиочастотной передачи для каждого из поддерживаемых этим стандартом типов модуляции. Эти требования используются для ограничения помех, вносимых устройством 802.11 в каналы, смежные с каналом, на котором оно работает. Поскольку радиочастотные каналы не имеют точных границ, желательно, чтобы устройства 802.11 использовали фильтрацию и/или другие методы минимизации радиочастотной энергии, излучаемой при передаче за пределами своего рабочего канала. И хотя эти «внеканальные» помехи сведены к минимуму, они не могут быть нулевыми.

В стандарте 802.11 (и/или его поправках) определены следующие маски спектра передачи:



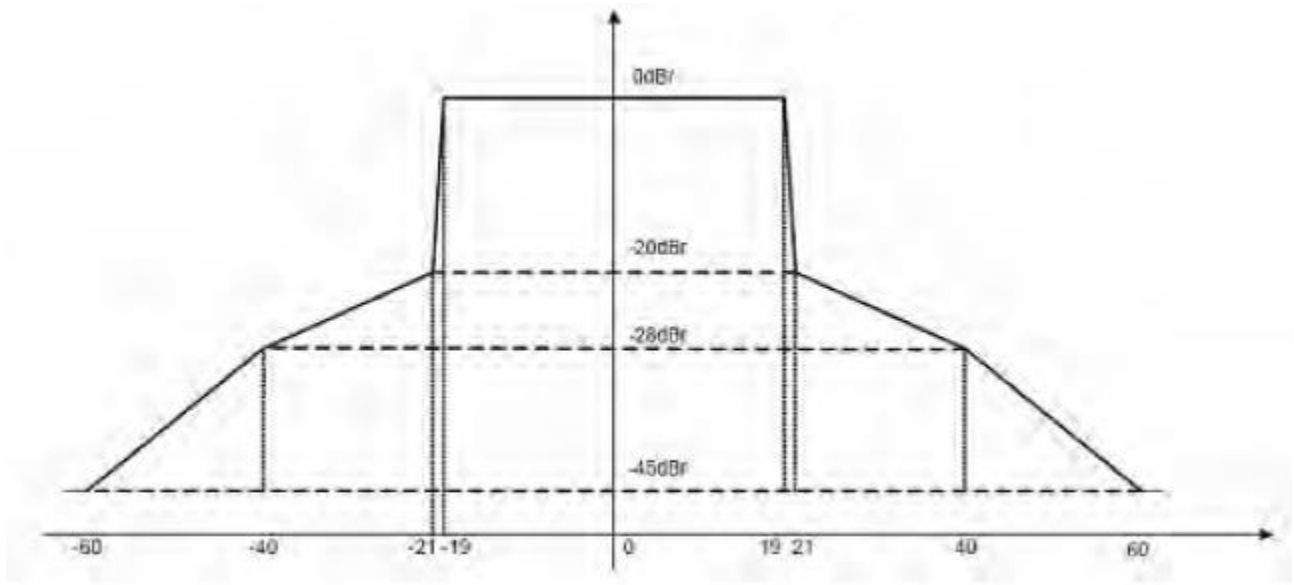
Transmit spectrum mask	Маска спектра передачи
Unfiltered Sinx/x	Sinx/x без фильтрации
MHz	МГц
dBr	дБп

Маска спектра передачи для 802.11b



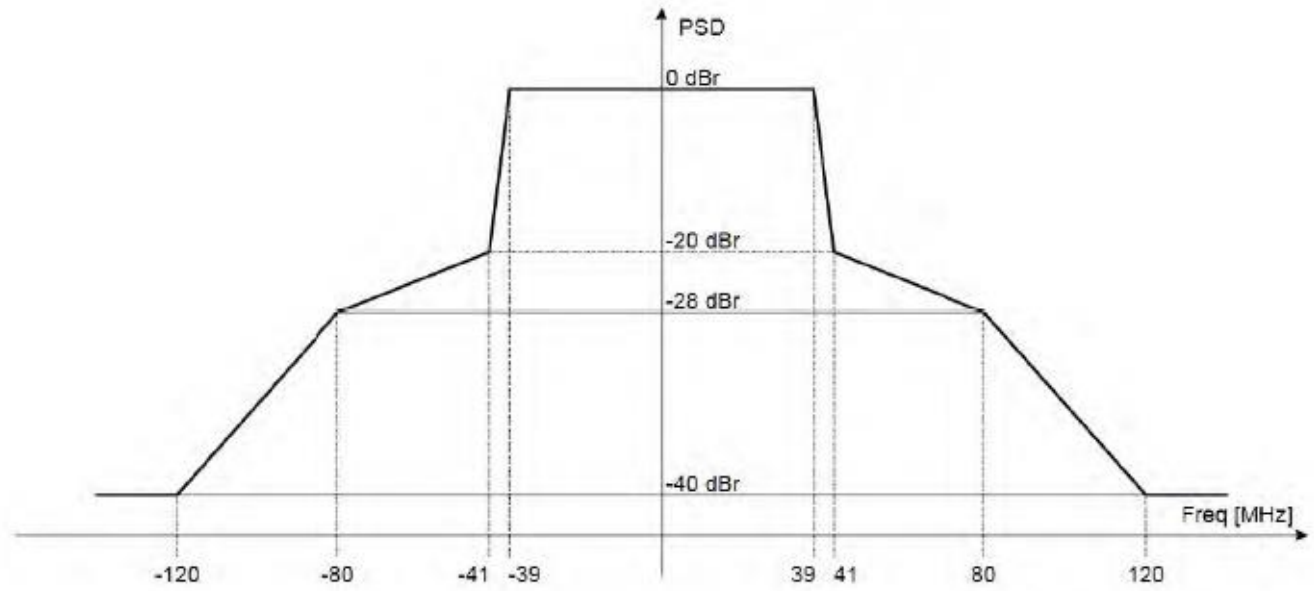
Power Spectral Density (dB)	Спектральная плотность мощности (дБ)
Transmit Spectrum Mask (not to scale)	Маска спектра передачи (не для масштабирования)
Typical Signal Spectrum (an example)	Типовой спектр сигнала (пример)
Frequency (MHz)	Частота (МГц)
dBr	дБп

Маска спектра передачи для 802.11a/g (20 МГц)



dBr	дБп

Маска спектра передачи для 802.11n (40 МГц)



Freq (MHz)	Частота (МГц)
dBr	дБп

Маска спектра передачи для 802.11ac (80 МГц)

Как показано на рисунках выше, устройству стандарта 802.11 разрешено при передаче вносить от -28 до -50 дБп (децибел относительно пикового уровня) на соседних каналах. При передаче в канале 40 МГц диапазона 2,4 ГГц радиочастотная энергия может присутствовать на расстоянии до 11 каналов от центральной частоты.

Приложение AirMagnet WiFi Analyzer использует эти спектральные свойства устройств 802.11 для определения количества помех, которые конкретное устройство вносит в определенный (логический) канал.

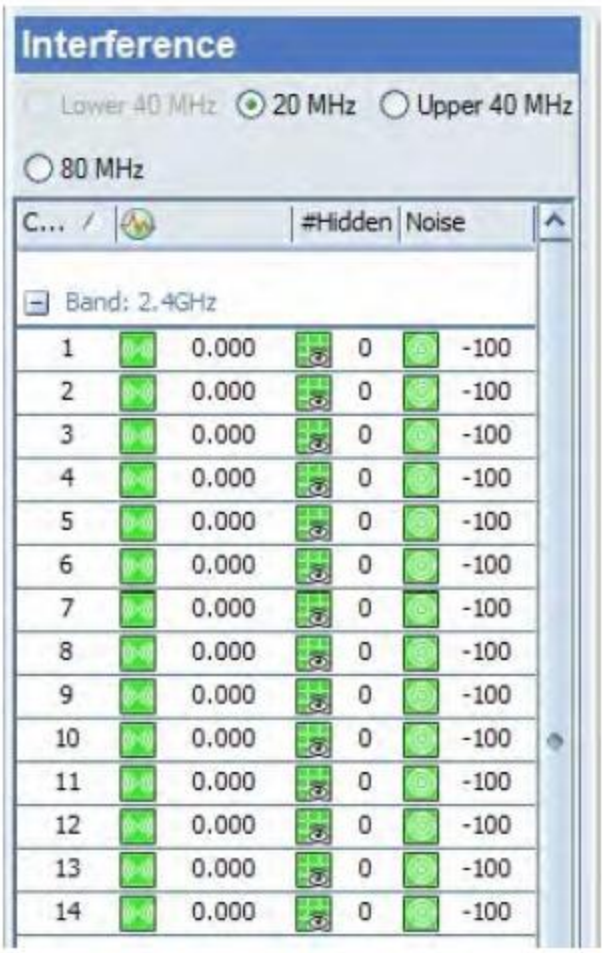
При расчете оценки помех учитывается следующее:

- «Спектральное расстояние» между рассматриваемым каналом и рабочим каналом устройства (включая ширину каждого канала).
- Вызваны ли помехи от устройства (в канал) модулированным спектром (то есть в пределах ширины рабочего канала устройства) или «утечкой» за пределы модулированной части передачи.
- RSSI (мощность сигнала) устройства.
- Текущее «использование полосы пропускания» устройства; то есть, как часто оно в настоящий момент осуществляет передачу.

После выполнения расчетов на основе описанных выше данных оценка помех нормализуется, масштабируется (и, возможно, ограничивается) для каждого устройства, что позволяет обеспечить определенную согласованность с предыдущими версиями продукта.
Следует отметить, что таким образом «загруженная» точка доступа на канале 6 с очень высоким уровнем сигнала может вносить больше помех в канал 1, чем менее загруженная точка доступа на канале 3, но с более слабым сигналом (из точки захвата).
В списке создающих помехи устройств, отображаемых на экране Interference (Помехи), различаются вклады модулированных ( ) и немодулированных ( ) помех. Обратитесь к разделу «Экран Interference (Помехи)».

Статистика помех по каналам

В левой части экрана Interference (Помехи) отображается статистика помех по каналам. Здесь предоставлен краткий обзор общего состояния помех на каждом доступном канале, что позволяет легко и быстро идентифицировать канал или каналы, требующие внимания.
В зависимости от выбранного канала и возможностей адаптера (802.11a/b/g/n/ac) для выбора желаемой ширины канала используются переключатели вверху (Lower 40 MHz, 20 MHz, Upper 40 MHz и 80 MHz).



Эта часть экрана содержит четыре столбца данных (слева направо):

- В первом столбце перечислены все доступные каналы по частотному диапазону 802.11 (2,4 ГГц и 5 ГГц). Чтобы показать или скрыть диапазоны, просто щелкайте кнопкой мыши на значках «+» или «-» в верхней части каждого раздела.

Примечание: Перечень доступных для выбора каналов зависит от выбранного типа среды передачи и страны или региона, в котором используется приложение AirMagnet WiFi Analyzer; распределение каналов в разных странах может отличаться.

- Во втором столбце отображаются оценки помех на каналах в режиме реального времени.

Примечание: Значки рядом с оценками помех имеют цветовую кодировку. Зеленый цвет предназначен для оценок помех, которые не считаются выходящими за пределы нормального уровня (0 – 4,999); желтый цвет для оценок помех, которые считаются «предупреждениями» (5 – 19,999); красный для сильных помех (20 и выше), которые требуют немедленного внимания. В приведенной ниже таблице представлен список пороговых значений цвета для каждого столбца.

Тип данных	Цветовые коды и помехи		
Помехи	0 - 5	5,01 - 20	20,01 или выше
Количество скрытых устройств	0 - 1	2 - 5	6 или выше
Количество источников шума	0 - 1	2 - 5	6 или выше

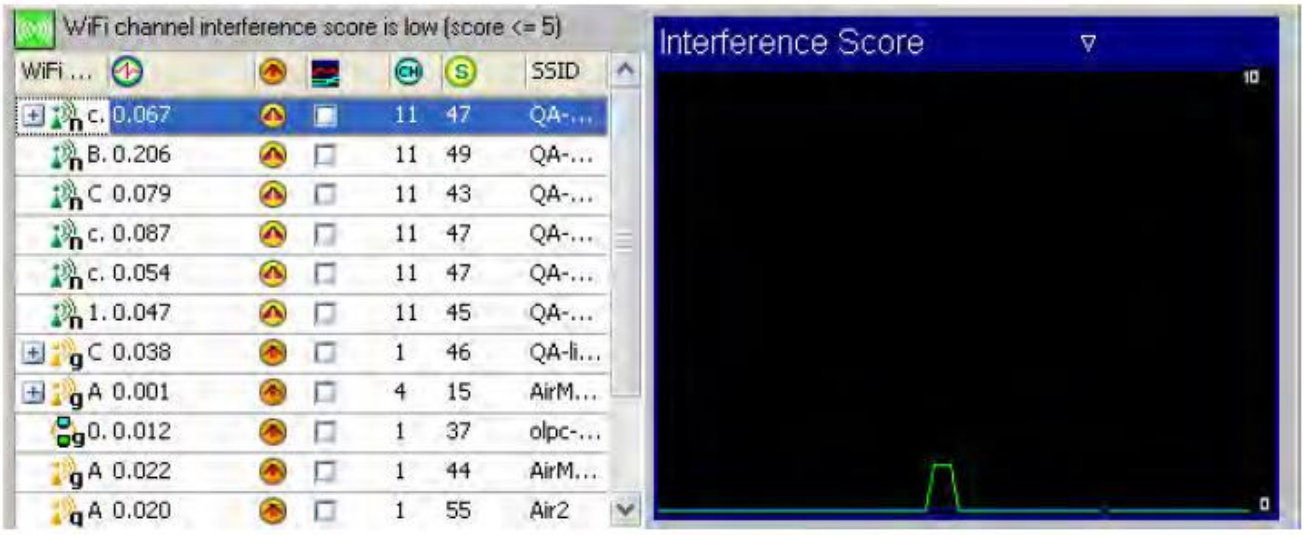
- В третьем столбце отображается количество скрытых устройств, обнаруженных на соответствующих каналах. Скрытые устройства могут вызывать помехи и коллизии трафика в сети, тем самым замедляя ее общую работу (более подробную информацию о скрытых устройствах можно найти в разделе «Обнаружена скрытая станция»).
- В четвертом столбце отображается количество обнаруженных источников помех от устройств, не относящихся к стандарту 802.11; эти устройства показаны на панели Hidden Devices (Скрытые устройства) справа.

Примечание: Столбец #Interferers будет содержать информацию только в том случае, если был интегрирован анализатор спектра AirMagnet и используется карта анализатора спектра AirMagnet (AirMagnet Spectrum Analyser).

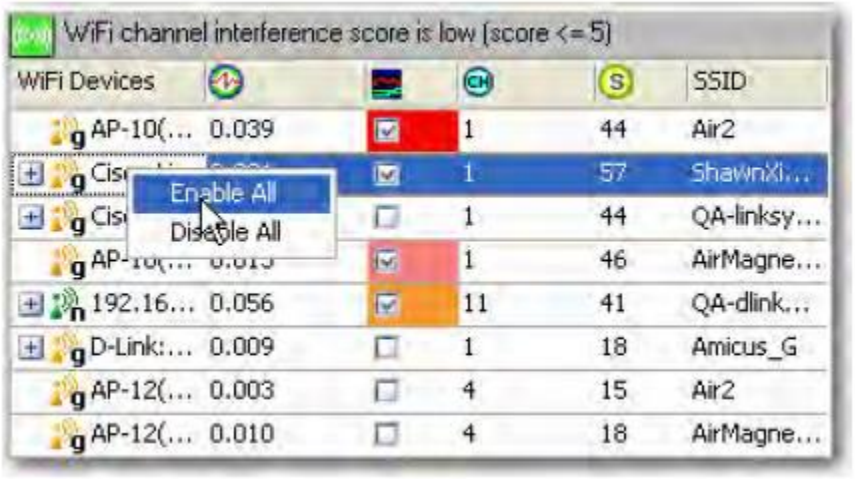
При выборе конкретного канала все области в правой части экрана Interference (Помехи) обновляются для отображения вызывающих помехи или шумы устройств, обнаруженных на этом канале. Обратитесь к панели Interference Analysis (Анализ помех).

Channel Interference (Помехи в канале)

Панель Channel Interference (Помехи в канале) состоит из двух частей. Левая часть представляет собой таблицу, в которой показаны все устройства, обнаруженные на выбранном канале, а также канал, оценка помех, мощность сигнала и идентификатор SSID каждого из устройств. Правая часть представляет собой график оценки помех (Interference Score), где оценки помех выбранных устройств отображаются в виде линейных диаграмм. Сообщение в верхней части таблицы информирует об общем состоянии радиочастотных помех на канале.



Для выбора устройств, которые будут отображаться на графике оценки помех, используйте поля в среднем столбце таблицы. Выберите нужное количество устройств (каждое выбранное устройство будет представлено линейной диаграммой уникального цвета). Кроме того, можно щелкнуть правой кнопкой мыши в любом месте таблицы и нажать Enable All (Включить все) во всплывающем меню для выбора всех устройств в списке.

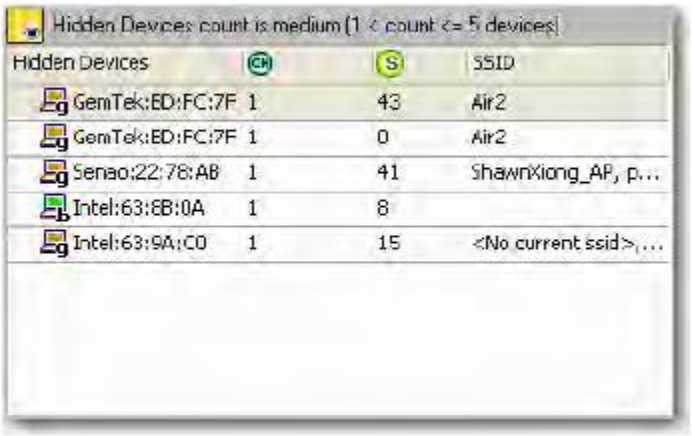


Однако одновременный выбор слишком большого количества устройств может привести к загромождению графика, который станет трудным в восприятии. Поэтому выбирайте только те устройства, которые действительно вас интересуют.

Примечание: Даже в случае выбора определенного канала на экране RF interference (Радиочастотные помехи) часто отображаются устройства с других каналов. Это связано с тем, что эти устройства также создают помехи на выбранном канале. Устройства на соседних каналах могут вызывать межканальные помехи.

Channel Hidden Device (Скрытые устройства на канале)

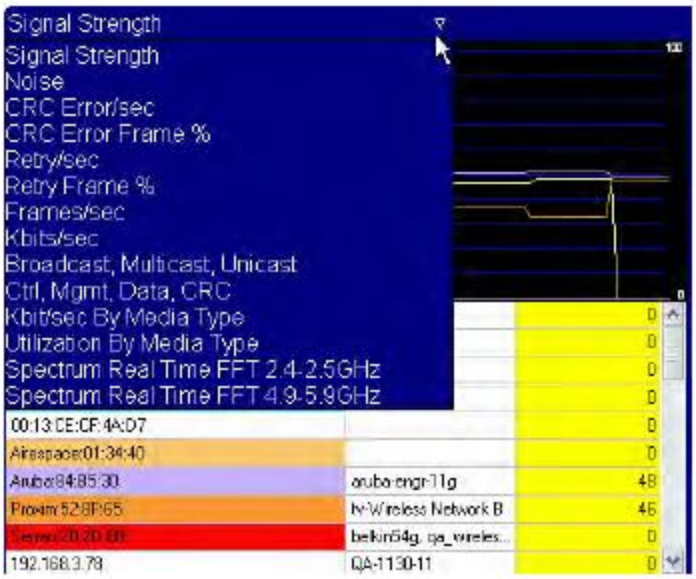
Панель Hidden Device (Скрытые устройства) расположена прямо под панелью устройств, создающих помехи в сети Wi-Fi. На ней отображаются все обнаруженные в вашей сети скрытые устройства, если таковые имеются. Там предоставлена такая информация, как имя устройства, канал, мощность сигнала и идентификатор SSID каждого обнаруженного скрытого устройства. Сообщение в верхней части этого раздела содержит информацию об общем количестве скрытых устройств, обнаруженных на канале.



Скрытые устройства являются проблемой, которая возникает, когда или где два беспроводных устройства (например, станции) не могут видеть друг друга напрямую (часто из-за расстояния между ними). Поскольку они не осведомлены друг о друге, то могут попытаться одновременно подключиться к одной и той же точке доступа между ними, что приведет к возникновению конфликтов в сети. Это заставит обе станции повторно передавать свои пакеты, и вызовет задержки сетевого трафика. Более подробную информацию о скрытых устройствах можно получить в разделе «Обнаружена скрытая станция» тревог AirWISE.

График данных канала

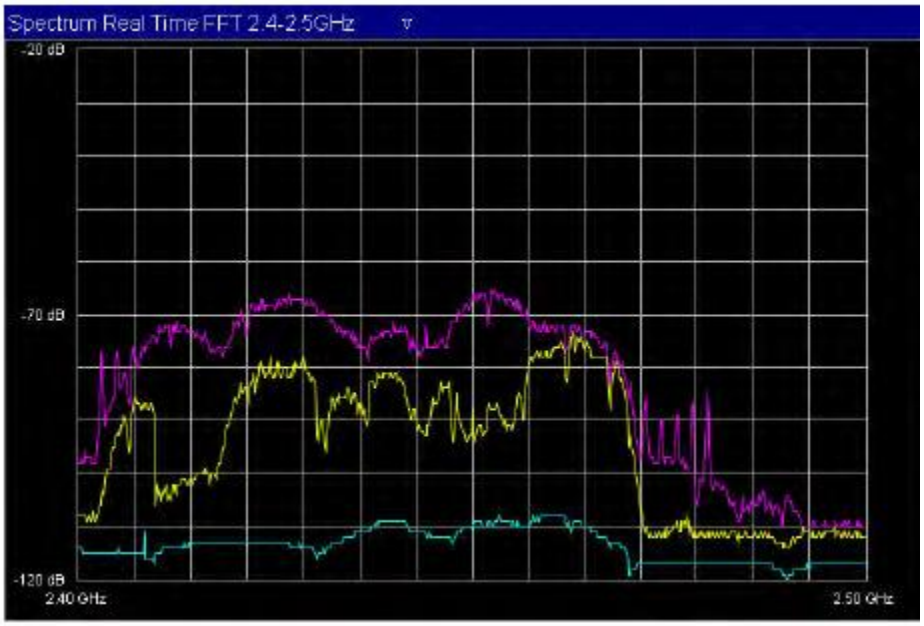
В этой части экрана различные типы данных о выбранном канале отображаются в виде линейных графиков. В верхней части этого экрана находится фильтр, позволяющий выбирать для графика более десятка типов данных. Это очень похоже на панель графика на экране Channel (Канал).



Примечание: В нижней части этой области экрана отображается информация, относящаяся к типу данных, выбранных из описанного выше фильтра данных. Цвета каждого устройства соответствуют цвету линий, которые будут отображаться на графике. Если какое-либо из устройств имеет справа нулевое значение, его график не появится.

Интеграция анализатора спектра AirMagnet Spectrum Analyzer

Когда используемое вами приложение AirMagnet WiFi Analyzer интегрировано с анализатором спектра (AirMagnet Spectrum Analyzer), на экране помех (Interference) под списком устройств также может отображаться третье поле. В нем показаны все обнаруженные вызывающие помехи устройства, не относящиеся к стандарту 802.11. К подобным устройствам могут относиться микроволновые печи, беспроводные телефоны, устройства Bluetooth, беспроводные камеры и т.д. При обнаружении таких устройств приложение AirMagnet WiFi Analyzer отправляет сигнал тревоги «Обнаружен источник помех, отличный от 802.11». Интеграция также позволит выбирать на панели графиков еще и график спектра.



Для включения анализатора спектра AirMagnet:

1. В главном меню нажмите Configure (Настроить) и откройте вкладку General (Общие).

2. Поставьте метку в поле Enable Spectrum Analyser (Включить анализатор спектра).
3. Для завершения нажмите OK.

Примечание: После включения опции AirMagnet Spectrum Analyzer для активации анализатора спектра необходимо перезапустить приложение AirMagnet WiFi Analyzer. Также убедитесь, что вы вставили адаптер анализатора спектра AirMagnet Spectrum Analyzer в слот для карт на своем портативном компьютере. После перезагрузки в нижней части экрана Interference (Помехи) приложения AirMagnet WiFi Analyzer будет отображаться новая панель с включенной опцией графика AirMagnet Spectrum Analyzer.

RF Spectrum Interferer (Радиочастотные источники помех)

На панели RF Spectrum Interferer (Радиочастотные источники помех) по мере обнаружения отображаются все устройства, не относящиеся к стандарту 802.11, которые влияют на производительность вашей сети.

RF Spectrum Interferer	Duty Cycle	Center Freq	Bandwidth	Power	Channel
Generic Wideband	6.20%	2450MHz	18MHz	-70.93dBm	6-10
Generic Wideband	24.14%	2453MHz	10MHz	-72.99dBm	8-10
Generic Wideband	22.24%	2454MHz	9MHz	-74.40dBm	8-10
Generic Wideband	26.57%	2454MHz	8MHz	-75.50dBm	8-10
Generic Wideband	36.97%	2453MHz	11MHz	-76.41dBm	8-10
Generic Wideband	37.07%	2452MHz	10MHz	-75.31dBm	8-10
Generic Wideband	39.34%	2452MHz	10MHz	-74.98dBm	8-10
Generic Wideband	39.02%	2453MHz	10MHz	-74.20dBm	8-10
Generic Wideband	39.14%	2453MHz	9MHz	-74.91dBm	8-10

В разделе под этой панелью отображается информация об обнаруженных источниках помех. Это дает представление о том, как источники помех влияют на производительность беспроводной сети.

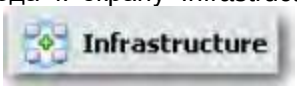
График анализатора спектра AirMagnet

Включение анализатора спектра AirMagnet позволяет просматривать график всего спектра 802.11 в диапазоне от 2,4 – 2,5 ГГц (для устройств 802.11b/g) до 4,9 – 5,0 ГГц (для устройств 802.11a и ac).
График анализатора спектра AirMagnet отображает диаграмму FFT (быстрое преобразование Фурье), который содержит три типа данных, представленных линиями разных цветов. Все эти данные кратко описаны в приведенной ниже таблице. Если необходимо получить дополнительную информацию об анализаторе спектра AirMagnet, обратитесь к «Руководству пользователя AirMagnet Spectrum Analyzer» или онлайн-справке в автономном приложении AirMagnet Spectrum Analyzer.

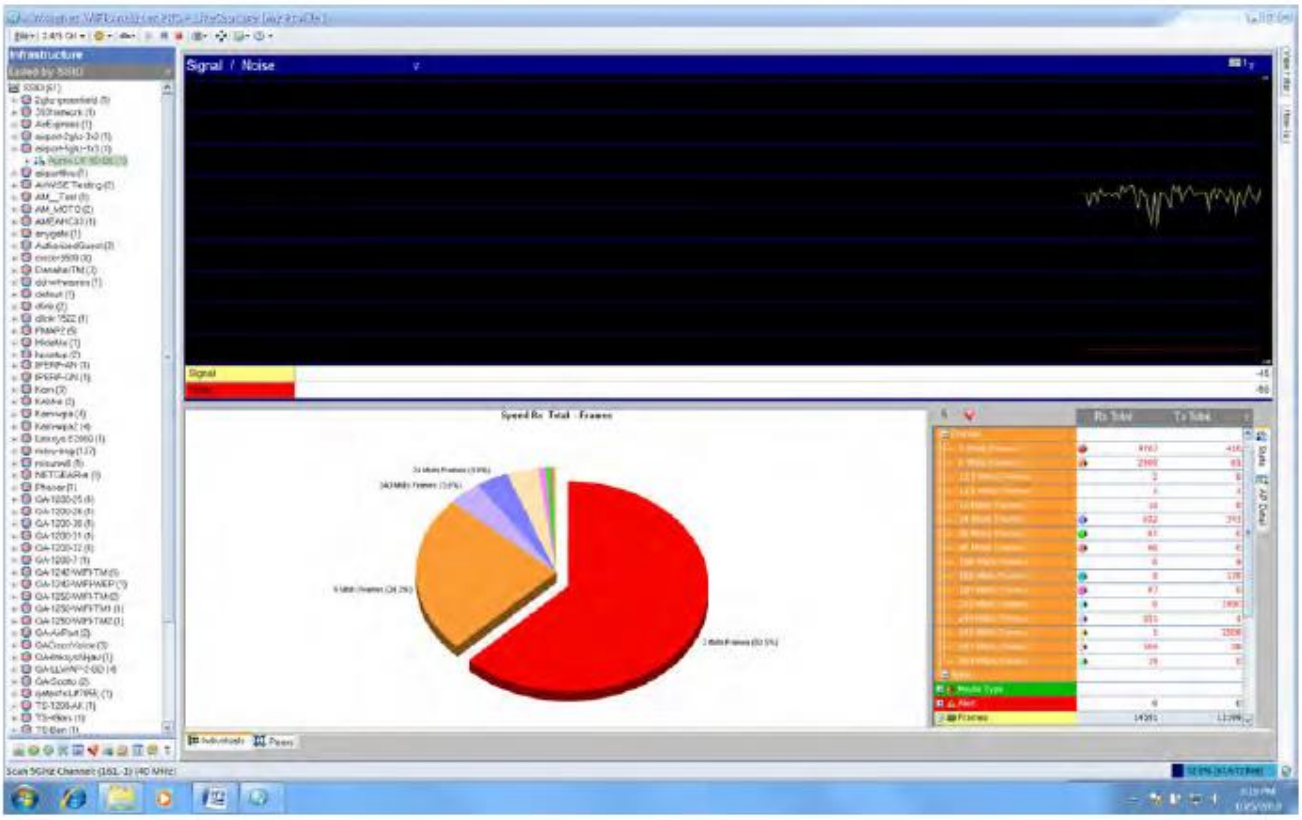
Цвет графика	Тип данных	Описание
Лиловый	Max Hold (Удержание максимального уровня)	Максимальное значение мощности, обнаруженное с момента запуска графика. Max Hold означает, что график сохраняет максимальное значение мощности, полученное до настоящего момента.
Желтый	Max (Максимальное значение)	Максимальное значение мощности, обнаруженное в течение последнего интервала измерения.
Голубой	Average (Среднее значение)	Среднее значение мощности, обнаруженное в течение последнего интервала измерения.

Экран Infrastructure (Инфраструктура)

Об экране Infrastructure (Инфраструктура)

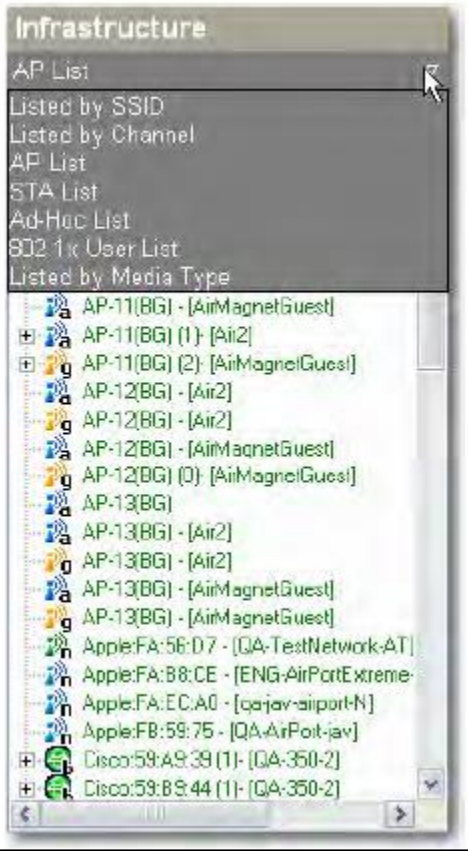
На экране Infrastructure (Инфраструктура) предоставлена исчерпывающая информация об инфраструктуре сети, которая позволяет проводить углубленный анализ данных всех устройств, составляющих сеть. Для перехода к экрану Infrastructure (Инфраструктура) в любой момент можно щелкнуть кнопкой мыши на 

на панели навигации. Экран Infrastructure (Инфраструктура) приложения AirMagnet WiFi Analyzer показан на рисунке ниже.



Опции просмотра экрана Infrastructure (Инфраструктура)

В левой части экрана Infrastructure (Инфраструктура) показаны компоненты, составляющие инфраструктуру вашей беспроводной сети. Там же представлен ряд опций для отображения компонентов сети. Для выбора нужной опции щелкните кнопкой мыши на направленной вниз стрелке; откроется разворачивающееся меню, в котором можно будет выбрать нужную опцию. По умолчанию на экране отображаются устройства по списку точек доступа.



Опция	Описание
Listed by SSID (Список по SSID)	Данная опция позволяет просматривать устройства (точки доступа и станции) по идентификатору SSID. Точки доступа, принадлежащие одному и тому же идентификатору SSID, группируются под этим SSID. Станции (если имеются), принадлежащие одной точке доступа, затем группируются вместе под этой точкой доступа (AP). Эта опция позволяет легко увидеть все идентификаторы SSID сети, а также то, какие точки доступа к каким SSID принадлежат.
Listed by Channel (Список по каналам)	Данная опция позволяет просматривать устройства (точки доступа и станции) по каналам. Точки доступа, работающие на одном канале, группируются под этим каналом. Станции (если имеются), принадлежащие одной точке доступа, затем группируются вместе под этой точкой доступа (AP). Эта опция позволяет легко увидеть все каналы, доступные в сети, а также то, какие точки доступа на каких каналах работают.
AP List (Список AP)	Эта опция позволяет просматривать все обнаруженные в сети точки доступа. Станции (если имеются), связанные с одной точкой доступа, затем группируются вместе под этой точкой доступа (AP).
STA List (Список станций)	Данная опция позволяет увидеть все обнаруженные в сети станции. Значок «+» перед станцией указывает, что она связана с точкой доступа. Разверните эту запись, чтобы определить точку доступ. Интеллектуальные устройства обозначаются синим значком сотового телефона.
Ad-Hoc List (Список устройств Ad-Hoc)	Данная опция отображает все обнаруженные в сети станции Ad-Hoc, если таковые имеются.
802.1x User List (Список пользователей 802.1x)	Данная опция отображает устройства (точки доступа и станции), использующие стандарт 802.1x.
Listed by Media Type (Список по типу среды)	Данная опция отображает точки доступа по типу среды 802.11 (то есть 802.11a, b, g, n и ac).

Примечание: Как видно на экране, все идентификаторы устройств (то есть их имена, IP-адреса, названия производителей и т.д.) имеют цветовую кодировку. Каждый цвет указывает на определенное рабочее состояние компонентов сети.
Примечание: Эта часть экрана Infrastructure (Инфраструктура) имеет контекстное меню, которое можно активировать щелчком правой кнопкой мыши на устройстве (например, точке доступа AP, станции STA и устройстве Ad Hoc). Некоторые опции всплывающего меню могут различаться в зависимости от типа устройства, на котором выполняется щелчок правой кнопкой мыши. Большинство параметров контекстного меню идентичны параметрам контекстного меню экрана Start (на панели анализа данных).

Цвет и рабочее состояние устройства

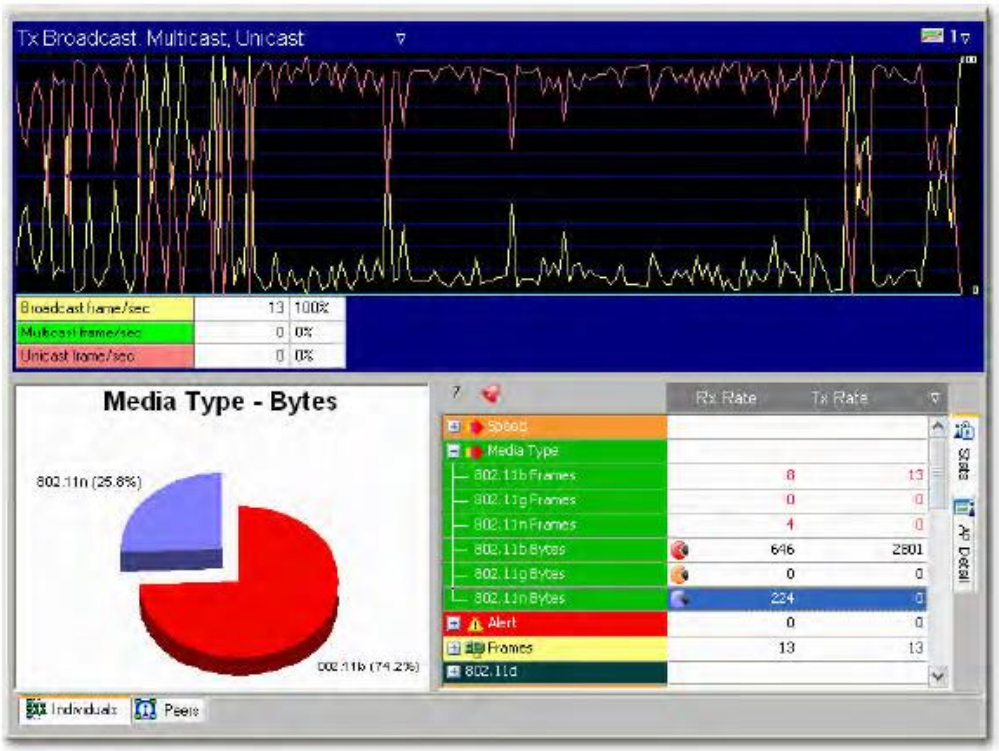
Все показанные в левой части экрана Infrastructure (Инфраструктура) сетевые устройства имеют цветовую кодировку, каждый цвет соответствует определенному рабочему состоянию, описанному в следующей таблице.

Цвет	Рабочее состояние устройства
Зеленый	Устройство было активно на протяжении последних 5 секунд.
Оранжевый	Устройство было неактивно в течение последних 5 - 60 секунд.
Красный	Устройство было неактивно в течение последних 60 - 300 секунд.
Серый	Устройство было неактивно в течение более 300 секунд.

Примечание: Описанная здесь цветовая схема применима только к именам устройств. Ее не следует путать с цветовой схемой, используемой на иконках устройств (то есть точек доступа AP, станций STA и устройств Ad Hoc), которая указывает на протоколы 802.11 (то есть 802.11a/b/g/n/ac) и/или частотные диапазоны (то есть 2,4 ГГц или 5 ГГц), используемые устройствами.

Анализ данных об отдельных устройствах

При выборе вкладки Individuals (Отдельные устройства) экран Infrastructure (Инфраструктура) позволяет просматривать и анализировать различные сетевые данные о любых конкретных устройствах, обнаруженных в сети. Все, что нужно сделать, это выбрать отдельное устройство (точку доступа, станцию и т.д.) на левой стороне экрана, а затем использовать инструменты на его правой стороне для просмотра и анализа различных сетевых данных, связанных с этим устройством.

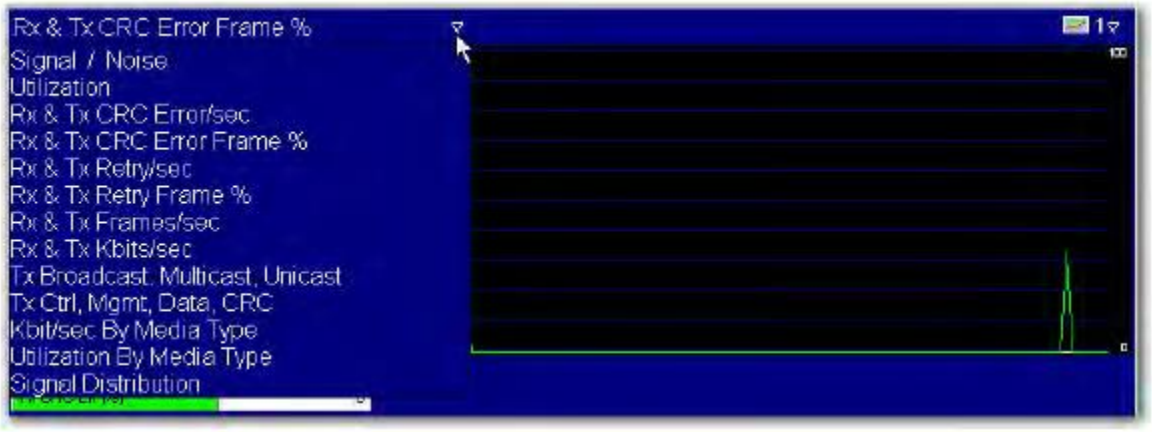


Как видно на рисунке, экран Infrastructure > Individuals (Инфраструктура > Отдельные устройства) содержит следующие компоненты пользовательского интерфейса, которые позволяют просматривать и анализировать сетевые данные, связанные с выбранным устройством:

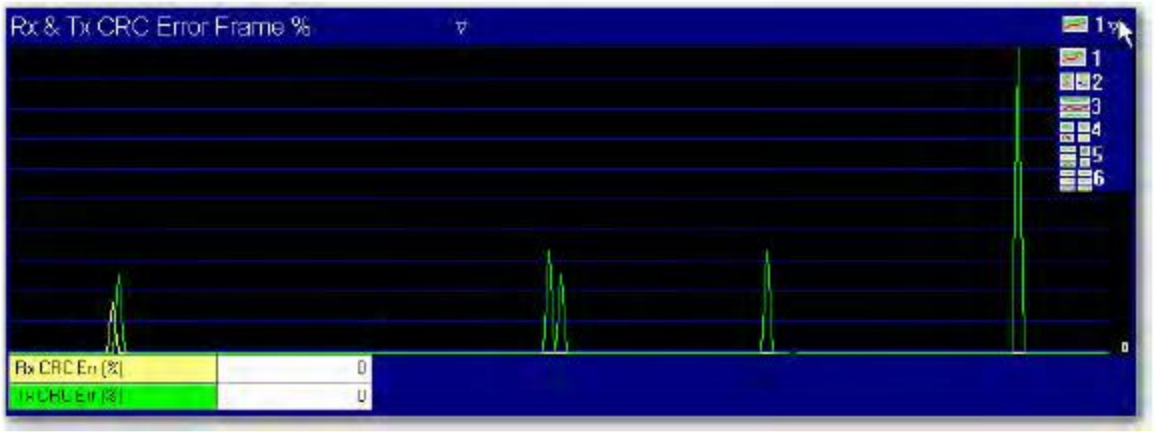
График данных

Верхняя часть экрана представляет собой панель, которая позволяет просматривать данные о выбранном устройстве в виде линейного графика. В этой части экрана представлены следующие инструменты просмотра и анализа данных, относящихся к выбранному устройству:

- Фильтр данных – Расположен в верхнем левом углу панели графика. Фильтр данных содержит более дюжины параметров фильтрации данных для графика. Щелкните кнопкой мыши на направленной вниз стрелке и выберите нужную опцию в разворачивающемся меню.



- Фильтр графика – Расположен в правом верхнем углу панели графиков. Фильтр графика позволяет выбрать количество графиков, которое будет отображаться одновременно. Щелкните кнопкой мыши на направленной вниз стрелке и выберите нужную опцию в разворачивающемся меню.



- Сводка данных – Расположена в нижнем левом углу панели графика. Содержание сводки данных зависит от опции, выбранной в фильтре данных (выше), и предоставляет цифровую сводку данных, отображаемых на графике.

Анализ данных

В нижней части экрана Infrastructure > Individuals (Инфраструктура > Отдельные устройства) можно просматривать и анализировать различные данные, касающиеся выбранного на левой стороне экрана устройства. Вдоль правого края экрана расположены две вкладки:

- Stats (Статистика) – Показывает статистические данные о выбранном устройстве в пяти категориях: Speed (Скорость), Media Type (Тип среды), Alerts (Тревоги), Frames (кадры), 802.11d и 802.11h. На экране отображаются два столбца данных для каждой категории, которые можно фильтровать с помощью фильтра в верхнем левом углу этого раздела. Чтобы развернуть или свернуть каждую категорию, щелкните кнопкой мыши на значке «+» или «-». Выбор записи в развернутой категории позволяет обновить содержимое круговой диаграммы слева.

Примечание: На круговой диаграмме отображаются только записи, отмеченные небольшими значками круговой диаграммы. Также, если в выбранной категории нет данных, диаграмма будет пустой.

- AP/Station Details (Сведения о точке доступа/станции) – Отображается подробная информация о выбранном устройстве.

Примечание: Эта вкладка помечена как AP Details (Сведения о точке доступа), если выбрана точка доступа, и Station Details (Сведения о станции), если выбрана станция. Этот раздел не влияет на круговую диаграмму слева.

- Alarm Count (Счетчик тревог) – Значение рядом со иконкой тревоги в верхней части этого раздела указывает общее количество сигналов тревоги, которые были инициированы устройством.

Примечание: Щелчок кнопкой мыши на иконке сигнала тревоги напрямую открывает экран AirWISE, где можно провести подробный анализ сигнала тревоги.

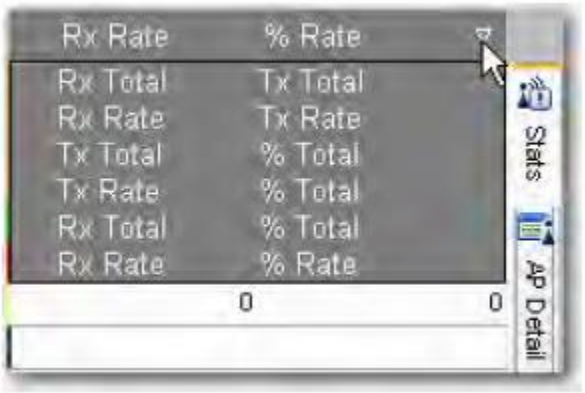
Информация о 802.11d/h

В двух дополнительных полях, которых нет на экране Channel (Канал), предоставляется информация об обнаруженных пакетах 802.11d или 11h.
Спецификация 802.11d очень похожа на спецификацию 802.11b, за исключением того, что 802.11d позволяет изменять свою конфигурацию на уровне MAC, гарантируя соответствие сети любым местным правилам и нормам. Системы, использующие стандарт 802.11d, могут изменять настройки частоты, уровни мощности и ряд других технических параметров. Это гарантирует, что стандарт 802.11d идеально подойдет для систем, которые будут использоваться в различных регионах мира, поскольку его можно адаптировать практически к любым требованиям. Приложение AirMagnet WiFi Analyzer позволяет просматривать настройки любого устройства, использующего стандарт 802.11d, что позволит быть уверенным в том, что все устройства используют одни и те же настройки.

Стандарт 802.11h устраняет ограничения, накладываемые на частоту 5 ГГц, используемую в настоящее время устройствами стандарта 802.11a. Международный союз электросвязи создал этот набор стандартов для предотвращения возможного возникновения помех между устройствами 802.11a и системами спутниковой связи. Приложение AirMagnet WiFi Analyzer обеспечивает простой просмотр всей информации, содержащейся в любых обнаруженных в вашей сети пакетах 802.11h.

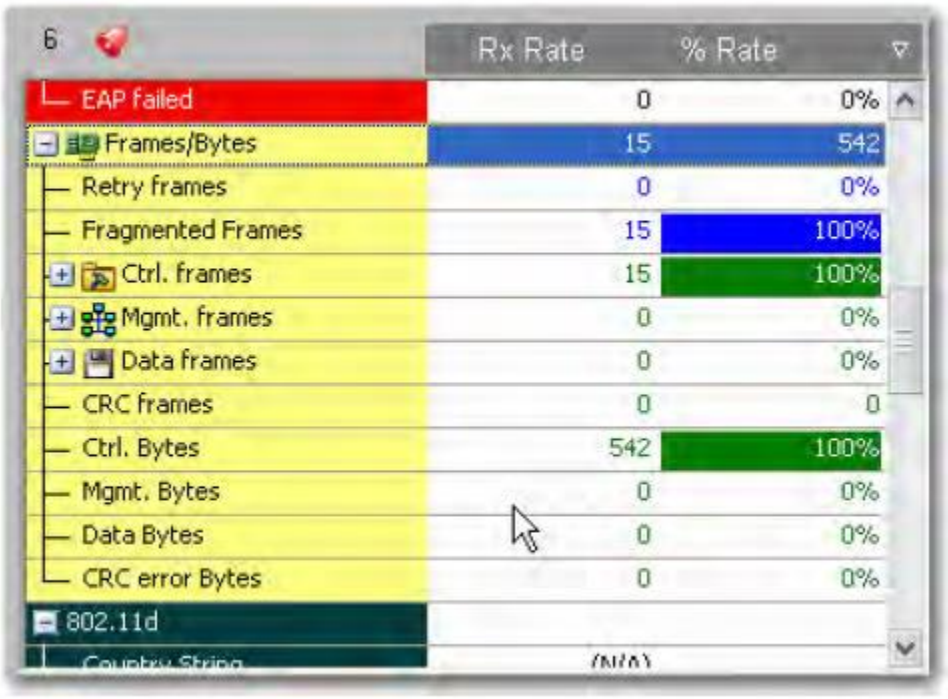
Фильтр статистики инфраструктуры

Открыв вкладку Stats (Статистика), в верхнем правом углу раздела анализа данных на экране Infrastructure (Инфраструктура) можно увидеть фильтр. Он содержит показанные в таблице ниже опции выбора данных. Для выбора любой из них щелкните кнопкой мыши на направленной вниз стрелке, чтобы открыть разворачивающийся список.



Левый столбец	Правый столбец	Описание
Rx Total	Tx Total	Всего принято; Всего передано (то есть общее количество полученных кадров/байтов по сравнению с общим количеством переданных кадров или байтов).
Rx Rate	Tx Rate	Скорость приема; Скорость передачи (то есть количество полученных кадров/байтов в секунду в сравнении с количеством переданных кадров/байтов в секунду).
Tx Total	% Total	Всего передано; Процент от общего числа (то есть общее количество переданных кадров/байтов определенного типа в сравнении с процентным выражением от общего числа всех переданных кадров/байтов).
Tx Rate	% Total	Скорость передачи; Процент от общего числа (то есть количество переданных кадров/байтов определенного типа в секунду в сравнении с процентным выражением от общего числа всех переданных кадров/байтов).
Rx Total	% Total	Всего принято; Процент от общего числа (то есть общее количество принятых кадров/байтов в сравнении с процентным выражением от общего числа всех принятых кадров/байтов).
Rx Rate	% Rate	Скорость приема; Процент от скорости (то есть количество принятых кадров/байтов определенного типа в сравнении с процентным выражением от общего числа всех принятых кадров/байтов).

Примечание: Слово «всего» (Total) относится либо к общему количеству кадров или байтов, тогда как слово «скорость» (Rate) подразумевает либо количество переданных или полученных кадров в секунду, либо количество переданных или полученных байтов в секунду. Кадр или байт могут быть далее разбиты на множество подкатегорий. Ниже приводится пример того, как интерпретировать статистику, отображаемую в этой части экрана Infrastructure (Инфраструктура).



Примечание. На приведенном выше рисунке показана статистика, отображаемая на экране при выборе фильтра Rx Rate -% Rate. Показанные на экране значения передают следующую информацию:

- Скорость приема составляет 15 кадров в секунду или 542 байта в секунду.
- Все 15 кадров, полученных в секунду, являются фрагментированными кадрами, которые также являются управляющими кадрами (Control Frame); таким образом, процентное выражение 100% для обоих.
- 15 кадров равны 542 байтам. Следовательно, значение Rx Rate составляет 542 байта в секунду, а значение %Rate равно 100% при выражении в байтах.

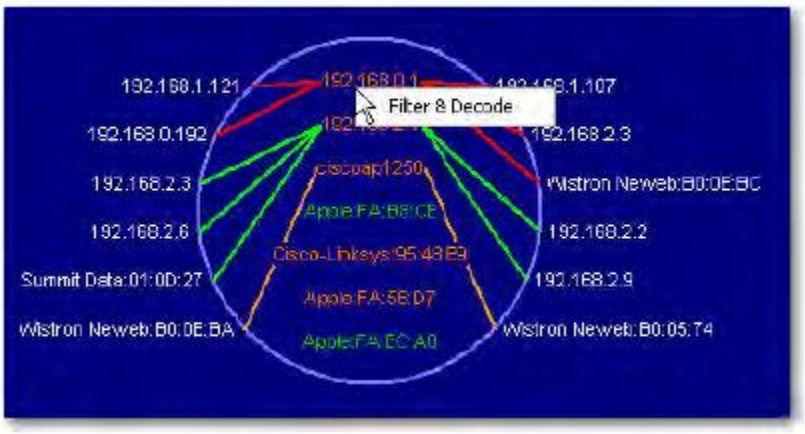
Анализ данных инфраструктуры

Правая часть экрана Infrastructure (Инфраструктура) позволяет просматривать и анализировать данные сетевой инфраструктуры на основе опции просмотра, выбранной в левой части экрана. Эта часть экрана также имеет две опции:

- Individuals (Отдельные устройства) - Позволяет просматривать и анализировать данные об отдельных компонентах инфраструктуры (точках доступа AP, станциях STA или устройствах Ad Hoc).
- Peers (Одноранговые узлы) - Позволяет просматривать соединения между выбранным устройством и другими устройствами.

Опции представлены двумя вкладками, расположенными в нижнем левом углу экрана. Переключение между двумя опциями осуществляется с помощью вкладок. По умолчанию при открытии экрана Infrastructure (Инфраструктура) автоматически выбирается вкладка Individual (Отдельное устройство).

Примечание: Две вкладки (Individual и Peers) отображаются непосредственно на экране, когда в качестве опции просмотра выбрано AP List (Список точек доступа), STA List (Список станций), Ad-Hoc List (Список устройств Ad-Hoc) или 802.1x User List (Список пользователей 802.1x). Однако в случае выбора в качестве параметра просмотра Listed by SSID (Список по SSID), Listed by Channel (Список по каналам) или Listed by Media Type (Список по типу среды) две вкладки не будут отображаться, если не выбрано конкретное устройство.
Примечание: Находясь на экране Infrastructure > Peers (Инфраструктура > Одноранговые узлы), можно перейти на экран Decodes (Декодирование), щелкнув правой кнопкой мыши на устройстве на графике и выбрав всплывающее меню Filter & Decode (Фильтрация и декодирование).

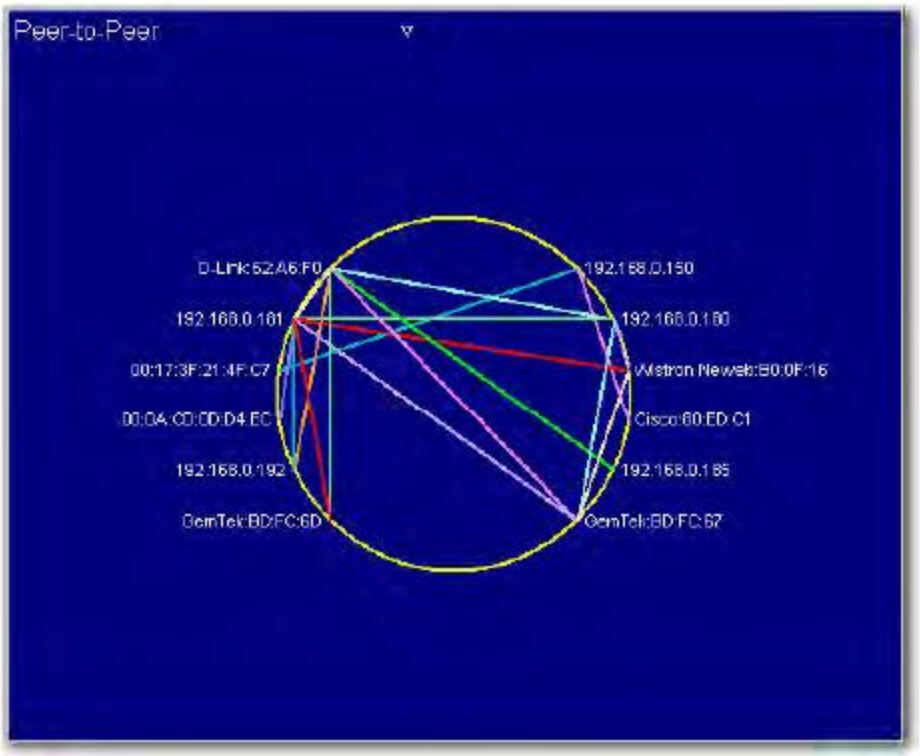


Анализ подключений устройств

Вкладка Peers (Одноранговые узлы) в нижнем левом углу этой части экрана Infrastructure (Инфраструктура) позволяет изменять отображение экрана Infrastructure для просмотра отображения. Это позволяет визуализировать соединение между выбранным устройством и другим устройством или устройствами на уровнях 2 и 3, когда они связываются друг с другом. Как показано в разворачивающемся списке в верхнем левом углу экрана графика, существует два сценария:

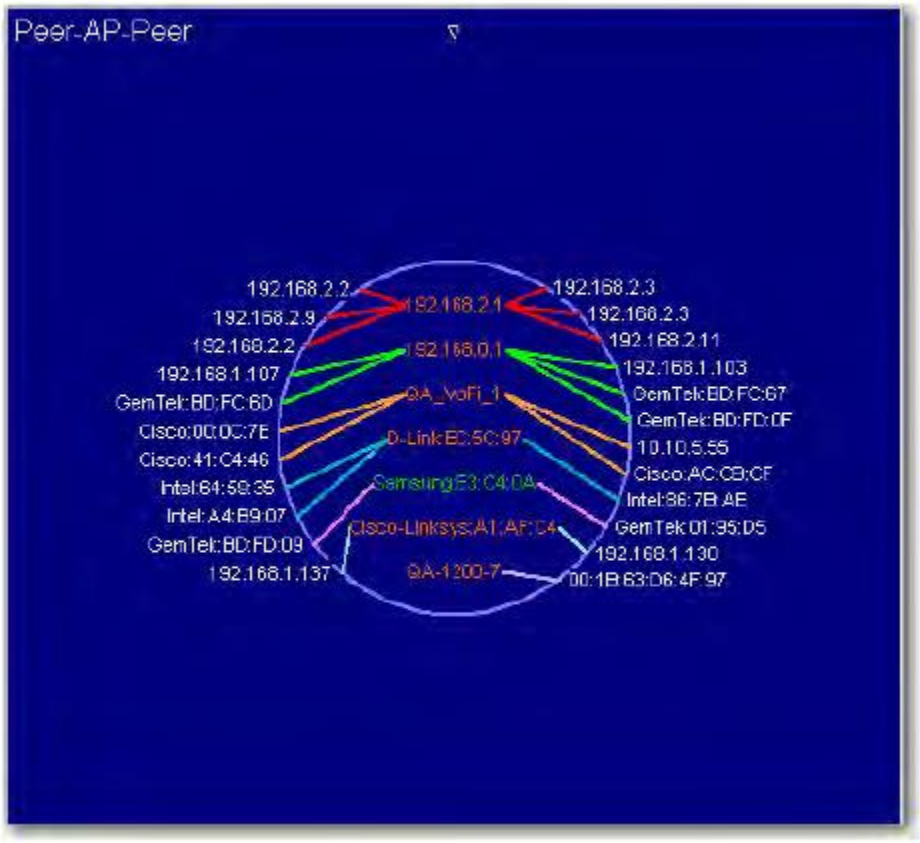
Peer-to-Peer (Одноранговое соединение)

График одноранговой сети показывает две беспроводные станции, напрямую связывающиеся друг с другом без помощи точки доступа. Все станции отмечены белым цветом; линии, соединяющие станции, имеют разные цвета, которые назначаются случайным образом для облегчения их различения.



Peer-AP-Peer (Соединение через точку доступа)

График Peer-AP-Peer показывает две беспроводные станции, связывающиеся друг с другом через точку доступа.



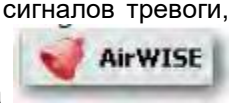
В сценарии Peer-AP-Peer устройства внутри круга являются точками доступа, а устройства за пределами круга - станциями. В то время как все станции отмечены белым цветом, независимо от используемых ими протоколов 802.11, точки доступа имеют цветовую кодировку, отражающую используемые ими протоколы 802.11:

- 802.11a – синий
- 802.11b – зеленый
- 802.11g - оранжевый
- 802.11n - зеленый (для 2,4 ГГц) и синий (для 5 ГГц)
- 802.11ac - лиловый

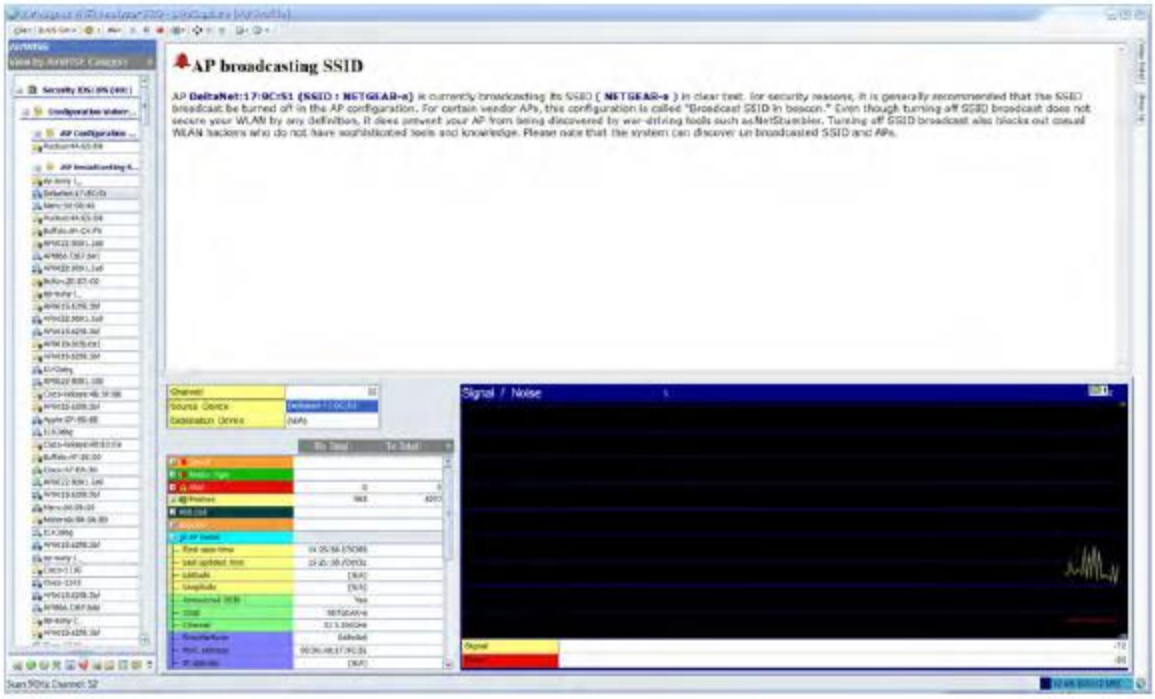
Линии между точками доступа и станциями также имеют разный цвет. Однако, в отличие от цветовой схемы, используемой для точек доступа, цвета линий назначаются случайным образом с единственной целью различать соединения различных точек доступа на экране.

Экран AirWISE

Об экране AirWISE

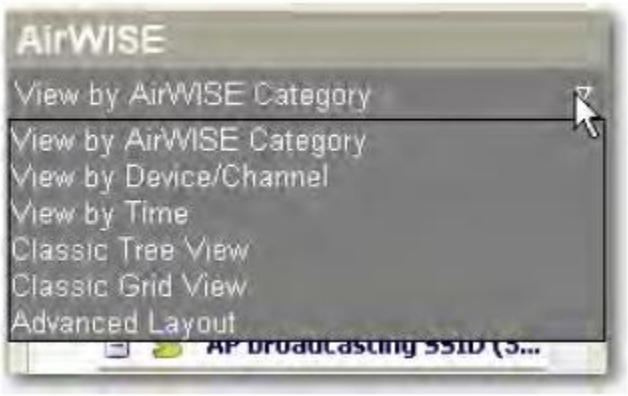
На экране AirWISE предоставляются различные средства для просмотра и анализа сигналов тревоги, возникающих в вашей сети. Для перехода к экрану AirWISE щелкните кнопкой мыши на 

на панели навигации. Экран AirWISE приложения AirMagnet WiFi Analyzer показан на рисунке ниже.



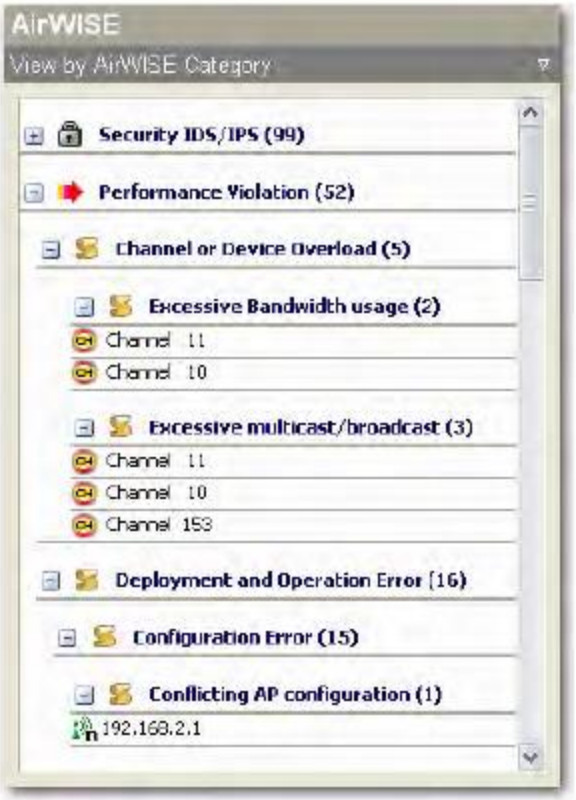
Опции просмотра экрана AirWISE

На левой стороне экрана AirWISE показаны сетевые сигналы тревоги, которые были захвачены приложением AirMagnet WiFi Analyzer с начала сеанса. Сигналы тревоги перечисляются в соответствии с выбранной пользователем опцией просмотра. Опцию просмотра можно выбрать с помощью фильтра, находящегося в верхней части экрана. Просто щелкните кнопкой мыши на стрелке, направленной вниз, и выберите нужный вариант в разворачивающемся списке.

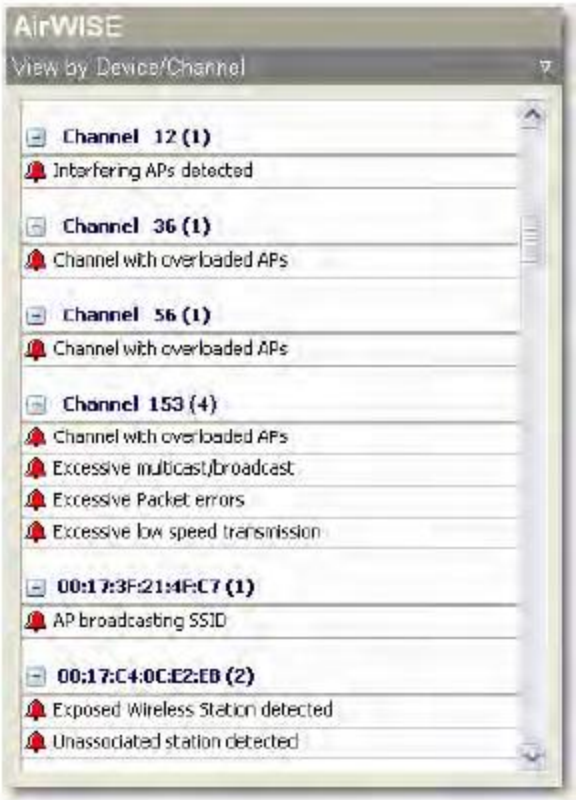


Экран AirWISE предоставляет следующие опции просмотра:

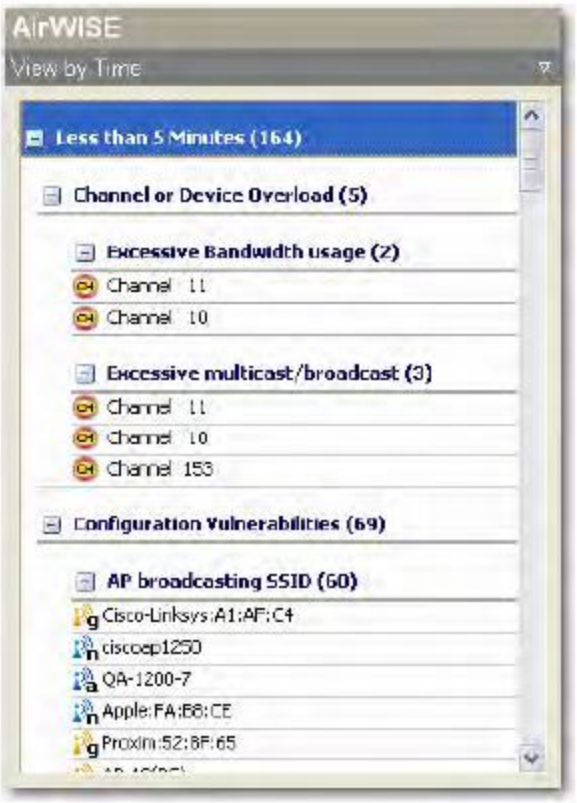
- View by AirWISE Category (Просмотр по категории AirWISE) – Эта опция позволяет отображать сигналы тревоги по структуре сетевой политики AirMagnet AirWISE.



- View by Device/Channel (Просмотр по устройству/каналу) – Эта опция позволяет отображать сигналы тревоги по каналу или по устройству.



View by Time (Просмотр по времени) – Эта опция позволяет отображать сигналы тревоги по времени их захвата. Сигналы тревоги, захваченные в течение определенного периода времени, объединяются в группы. В дальнейшем сигналы тревоги в этих временных рамках делятся по структуре сетевой политики AirWISE.

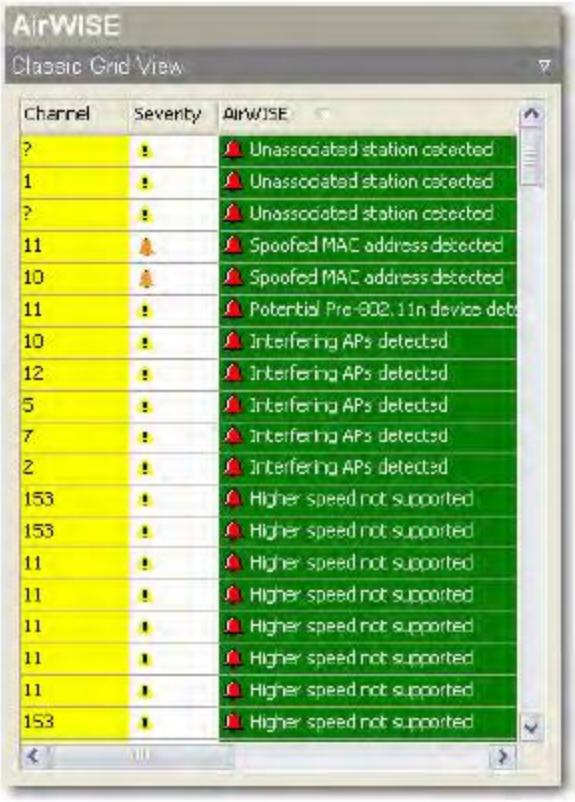


- Classic Tree View (Классическое древовидное представление) – Эта опция позволяет отображать аварийные сигналы с помощью классической древовидной структуры AirMagnet, которая основана на структуре сетевой политики AirWISE. Все сигналы тревоги, принадлежащие к одной и той же категории политики, группируются вместе. Также отображается уровень серьезности каждого сигнала тревоги.

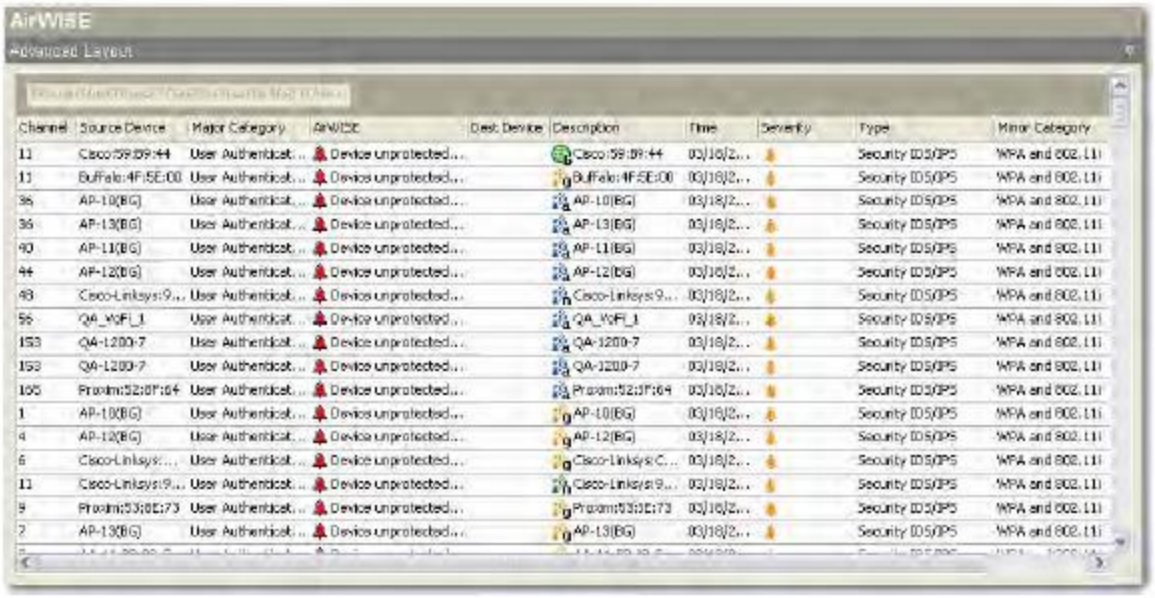
Степень серьезности сигнала тревоги обозначается иконкой перед ним, как показано в таблице ниже:

Иконка тревоги	Серьезность тревоги
	Критическая
	Срочная
	Предупреждение
	Информационная

- Classic Greed View (Классический вид сетки) – Эта опция позволяет отображать сигналы тревоги с использованием классической структуры сетки AirMagnet.



- Advanced Layout (Расширенный макет) – Данная опция позволяет настроить способ отображения сигналов тревоги на экране. Для ее использования может потребоваться растянуть правый край этой панели экрана вправо, чтобы отобразить все доступные параметры. Столбцы данных можно располагать в любом порядке, перетаскивая их в нужные места.



Управление списком сигналов тревоги

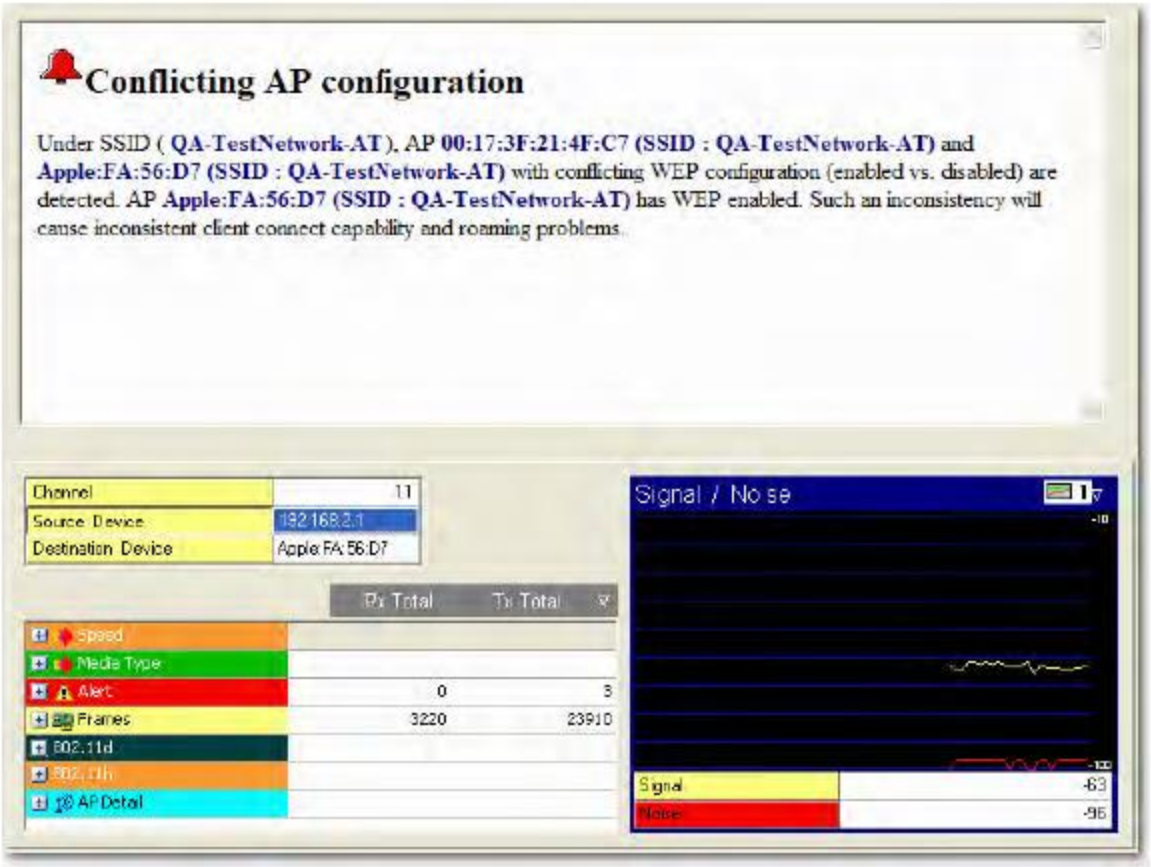
Приложение AirMagnet Wi-Fi Analyzer отображает все сигналы тревоги по мере их захвата. Сигналы тревоги отображаются на экране в порядке появления, причем самый старый отображается вверху списка. Для эффективного использовать места на экране можно удалять сигналы тревоги, особенно те, на которые уже отреагировали. Для этой цели предназначены два специальных инструмента на экране AirWISE

-  - Удаление выбранного сигнала тревоги (или верхнего сигнала в списке, если сигнал тревоги не выбран). Для удаления выделите соответствующий сигнал тревоги в левой части экрана (опции просмотра) и нажмите эту кнопку.
-  - Удаление всех сигналов тревоги, отображаемых в данный момент на экране. Чтобы удалить все сигналы тревоги на экране, нажмите эту кнопку.

Панель анализа сигналов тревоги экрана AirWISE

В правой части экрана AirWISE находится панель анализа сигналов тревоги, которая позволяет проводить углубленный анализ выбранного сигнала тревоги.

Примечание: Отображаемые на этой панели данные зависят от выбора, сделанного в дереве политик на левой стороне экрана. По мере углубления в структуру политик информация становится всё более конкретной.



Просмотр описания тревоги и совет эксперта

Как показано выше, верхняя правая часть экрана Advice (Совет) предоставляет подробное объяснение выбранной тревоги и рекомендации по предотвращению ее возникновения. Для просмотра всего совета целиком, возможно, понадобится использовать полосу прокрутки вдоль правого края экрана.

Анализ данных

В разделе Data Analysis (Анализ данных) отображается канал, на котором возникла тревога, а также исходный узел и узел назначения соединения. Это позволяет провести подробный анализ выбранного сигнала тревоги. Экран предоставляет два варианта отображения: Details (Подробности) и Graph (График). Первый представляет собой сводную таблицу данных с указанием скорости (Speed), предупреждения (Alert), кадров (Frames), управляющих кадров (Control Frames), кадров менеджмента (Management Frames), кадров данных (Data Frames) и сведений о точках доступа (AP Details) или сведений о станции (Station Detail). Второй обеспечивает графическое отображение данных в шести различных вариантах просмотра. Для переключения между двумя вариантами используйте вкладки вдоль правого края экрана. На приведенном ниже рисунке показан экран анализа данных при выборе вкладки Graph (График). Если разрешение экрана достаточно высокое или если сам экран достаточно широкий, содержимое каждой вкладки отображается на отдельном экране.

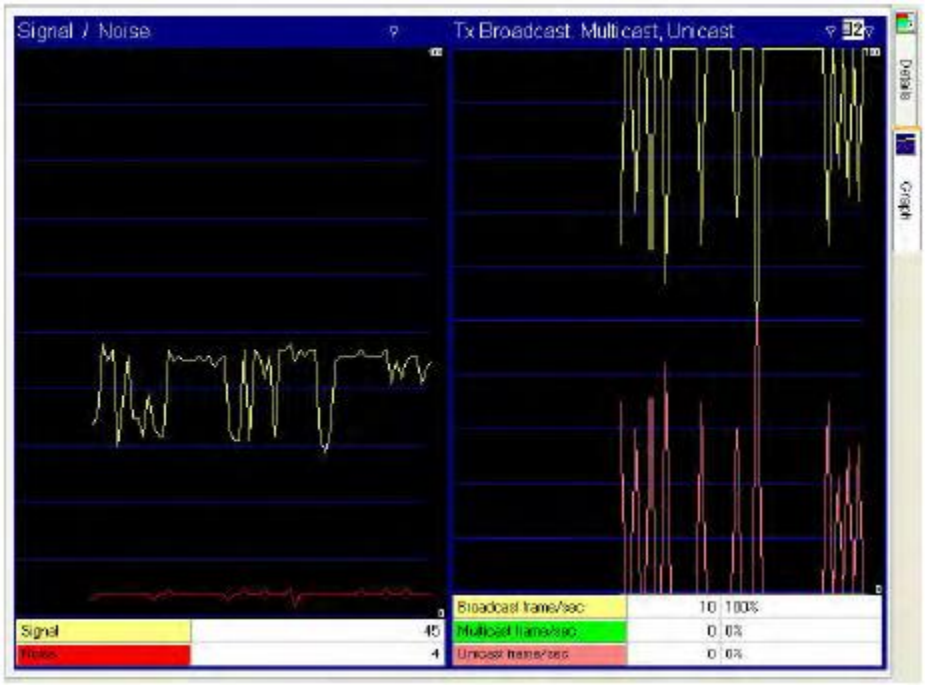
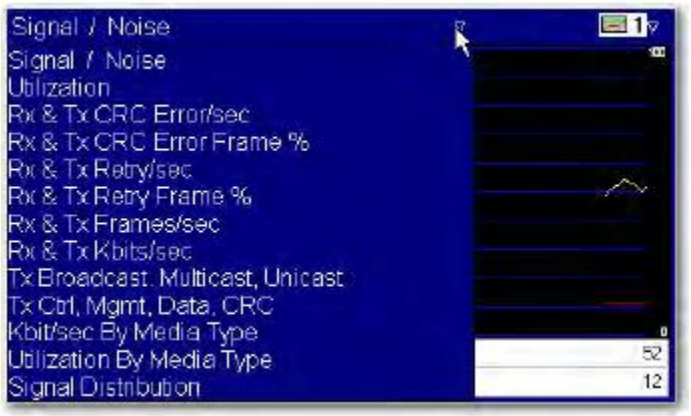
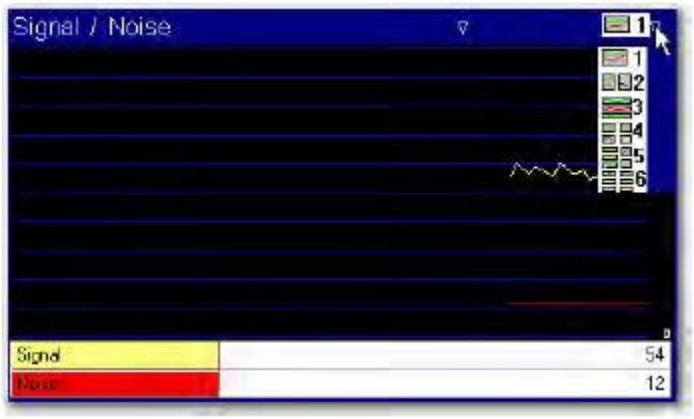


График данных на экране AirWISE

График данных находится в правом нижнем углу экрана AirWISE. Он позволяет просматривать и анализировать различные данные о канале или устройстве, задействованном в выбранной тревоге, в виде линейных графиков. В правом верхнем углу находится фильтр данных, который содержит все варианты данных и позволяет их выбирать. Щелкните кнопкой мыши на направленной вниз стрелке и выберите нужный вариант в разворачивающемся меню.



В верхнем левом углу находится фильтр графиков, который позволяет выбрать количество одновременно отображаемых на экране графиков. Щелкните кнопкой мыши на направленной вниз стрелке и выберите нужный вариант в разворачивающемся меню.



Примечание: Если выбрано конкретное устройство (то есть точка доступа, станция, устройство Ad-Hoc), на графике отображаются данные только для этого устройства. Если же выбран канал, на графике будут отображаться данные для всего канала.

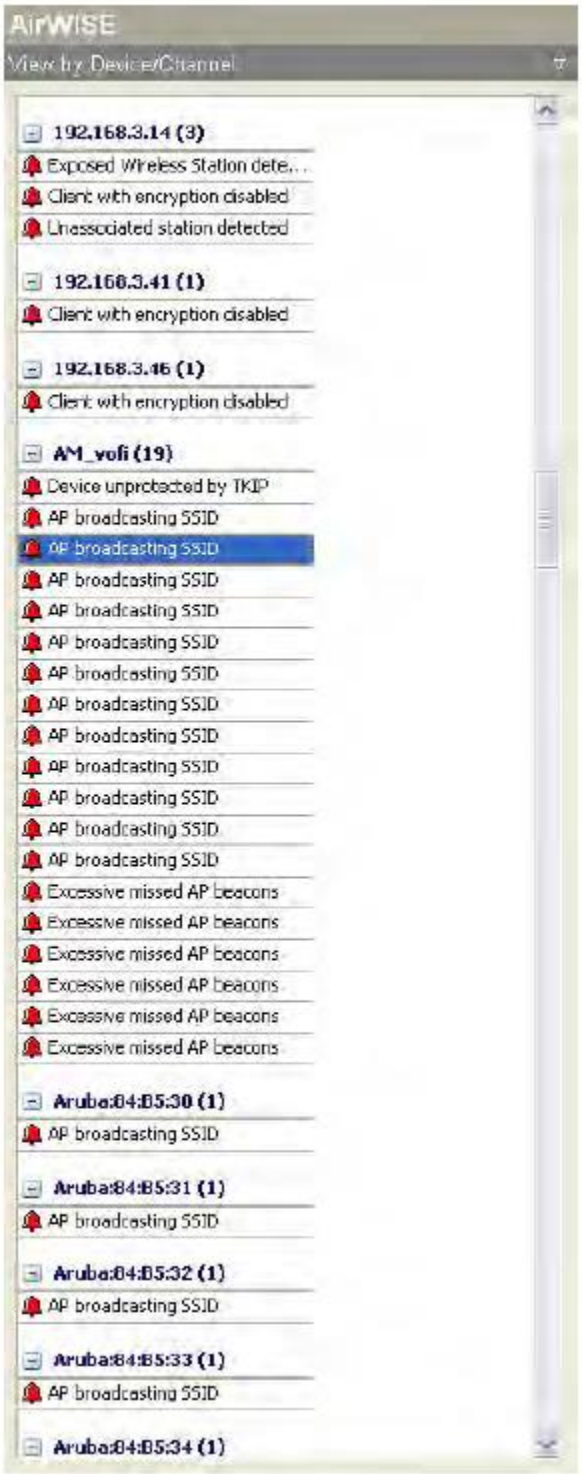
Просмотр всех сигналов тревоги для определенного устройства

Данная функция позволяет просматривать на одном экране все сигналы тревоги, генерируемые конкретным устройством. Выбор способа организации и просмотра сигналов тревоги по устройствам позволяет анализировать сигналы тревоги для различных устройств.

Для отображения всех сигналов тревоги, подаваемых определенным устройством:

1. В разделе Network Policy Hierarchy (Иерархия сетевых политик) выберите категорию политики и разверните ее до уровня тревоги.
2. Щелкните правой кнопкой мыши на тревоге и выберите во всплывающем меню View Device Alarms (Посмотреть тревоги устройства).

После щелчка кнопкой мыши на View Device Alarms (Посмотреть тревоги устройства) экран AirWISE обновится и отобразит всех сигналы тревоги, подаваемые одним и тем же устройством.



3. Для просмотра информации об устройстве и описания сигнала тревоги щелкайте кнопкой мыши на каждом сигнале тревоги.
4. Чтобы вернуться к общему экрану AirWISE, щелкните кнопкой мыши на направленной вниз стрелке фильтра над Network Policy Hierarchy (Иерархия сетевых политик) и выберите в разворачивающемся списке View by AirWISE Category (Просмотр по категории AirWISE).

Анализ данных канала или устройства

В нижней левой части панели анализа тревог находится раздел, содержащий исчерпывающую подробную информацию о выбранном канале, исходном устройстве и устройстве назначения. Смотрите раздел выше. Приведенные данные сгруппированы в семь категорий. Чтобы развернуть любую из них, щелкните кнопкой мыши на соответствующем значке «+».

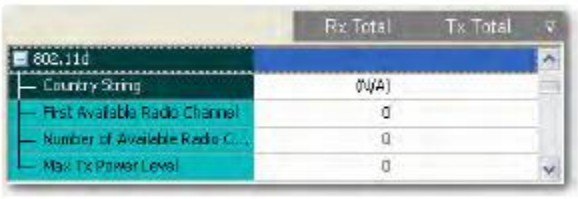
- Speed (Скорость) – Отображаются все доступные скорости передачи данных в кадрах или байтах на канале (если выбран канал) или скорости передачи данных, используемые устройством (если выделено исходное устройство или устройство назначения).

- Media Type (Тип среды) – Отображаются протоколы 802.11 (то есть 802.11a, 802.11b, 802.11g, 802.11n и 802.11 ac) в виде кадров и байтов, используемые на канале или выбранном исходном устройстве/устройстве назначения.

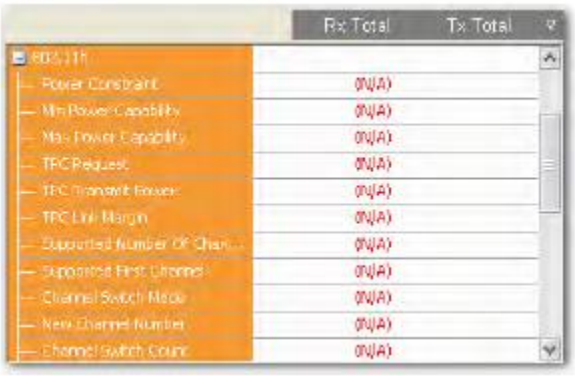
- Alert (Предупреждение) – Отображаются все типы данных предупреждений на канале или запускаемые выбранным устройством.

- Frames (Кадры) – Отображаются все типы данных кадров, включающие выбранный канал или устройство.

- 802.11d – Отображаются данные 802.11d о выбранном канале или устройстве.

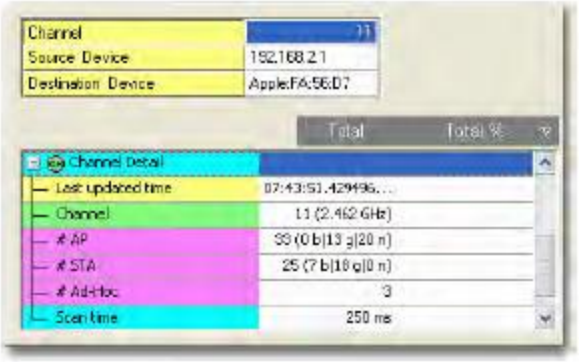


- 802.11h – Отображаются данные 802.11h о выбранном канале или устройстве.

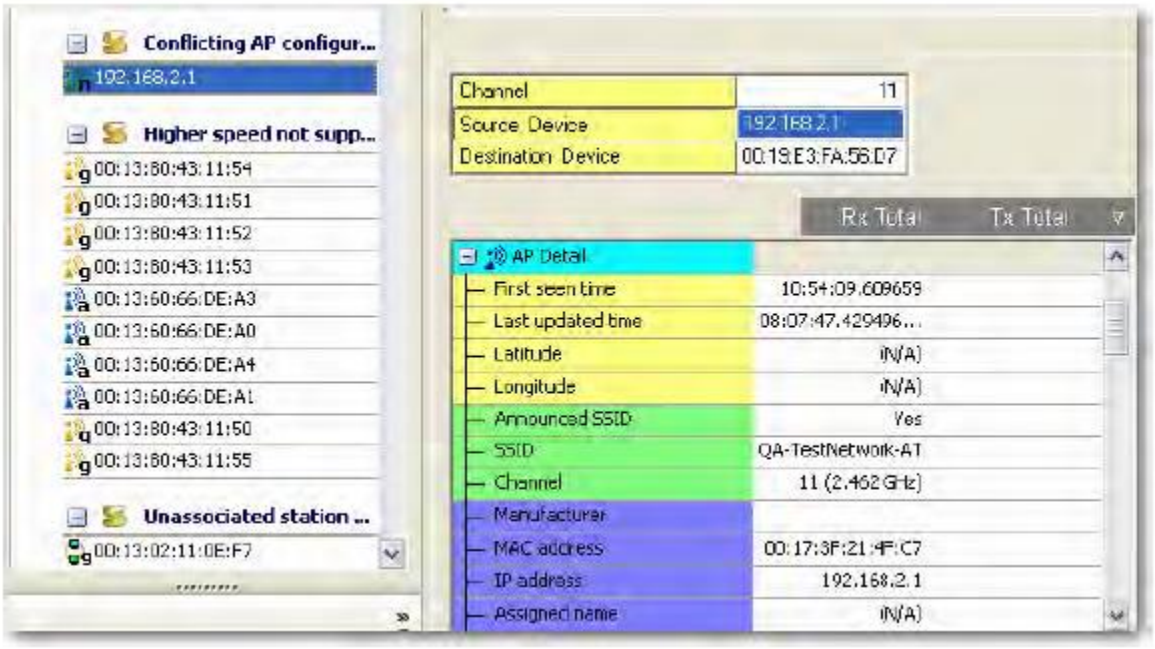


- Channel Detail (Сведения о канале) / AP Detail (Сведения о точке доступа) / Station Detail (Сведения о станции) – Отображается подробная информация о выбранном канале, точке доступа или станции. Название и содержимое этой папки зависят от выбора, сделанного в опции просмотра в левой части экрана и/или в разделе физической информации о тревоге выше.

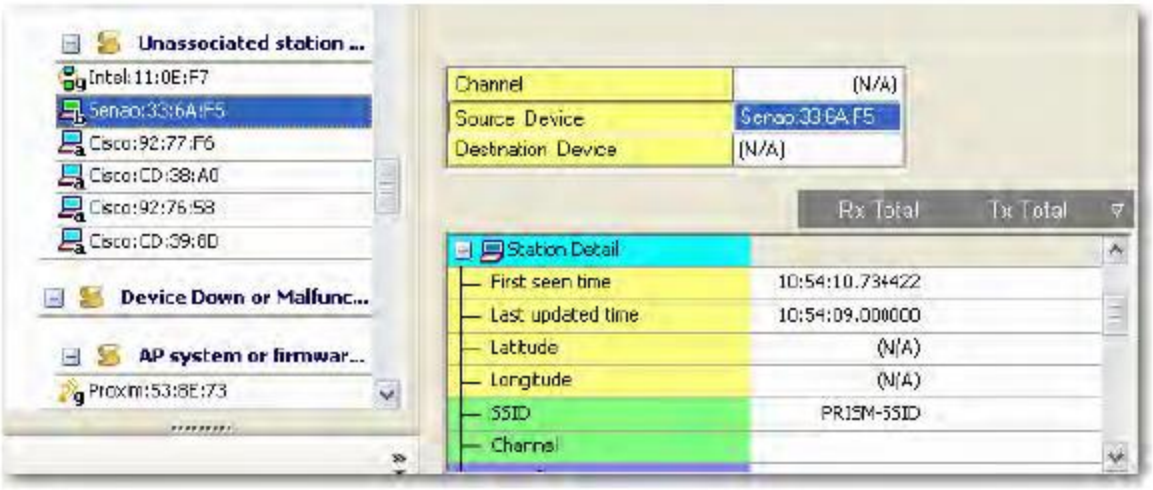
Channel Detail (Сведения о канале)



AP Detail (Сведения о точке доступа)



Station Detail (Сведения о станции)



Физическая информация о тревоге

Эта часть экрана AirWISE располагается в его середине слева прямо под описанием сигнала тревоги и предоставляет некоторую основную физическую информацию об устройстве, которое активировало выбранный сигнал тревоги.

- Channel (Канал) – Канал, на котором находилось устройство, активировавшее тревогу.
- Source Device (Исходное устройство) – Устройство (идентифицируемое по имени, IP-адресу и т.д.) на передающей стороне соединения.
- Destination Device (Устройство назначения) – Устройство (идентифицируемое по имени, IP-адресу и т.д.) на принимающей стороне соединения.

Примечание: Если устройство (точка доступа, станция и т.д.) выбирается в опциях просмотра с левой стороны, в этой части экрана отображается канал, на котором работает устройство, и доступная информация (имя, IP-адрес и т.д.) об исходном устройстве и устройстве назначения. Однако если канал выбран в опциях просмотра, то будет показан только канал; поля исходного устройства и устройства назначения будут пусты (то есть N/A). Выделенное (щелчком кнопкой мыши) в этой части экрана отражается в разделе «Анализ данных канала или устройства». Если выделен канал, то все, что будет показано в разделе ниже, относится ко всему каналу; если же выделено исходное устройство, то все, что показано в разделе ниже, относится к этому исходному устройству и так далее.

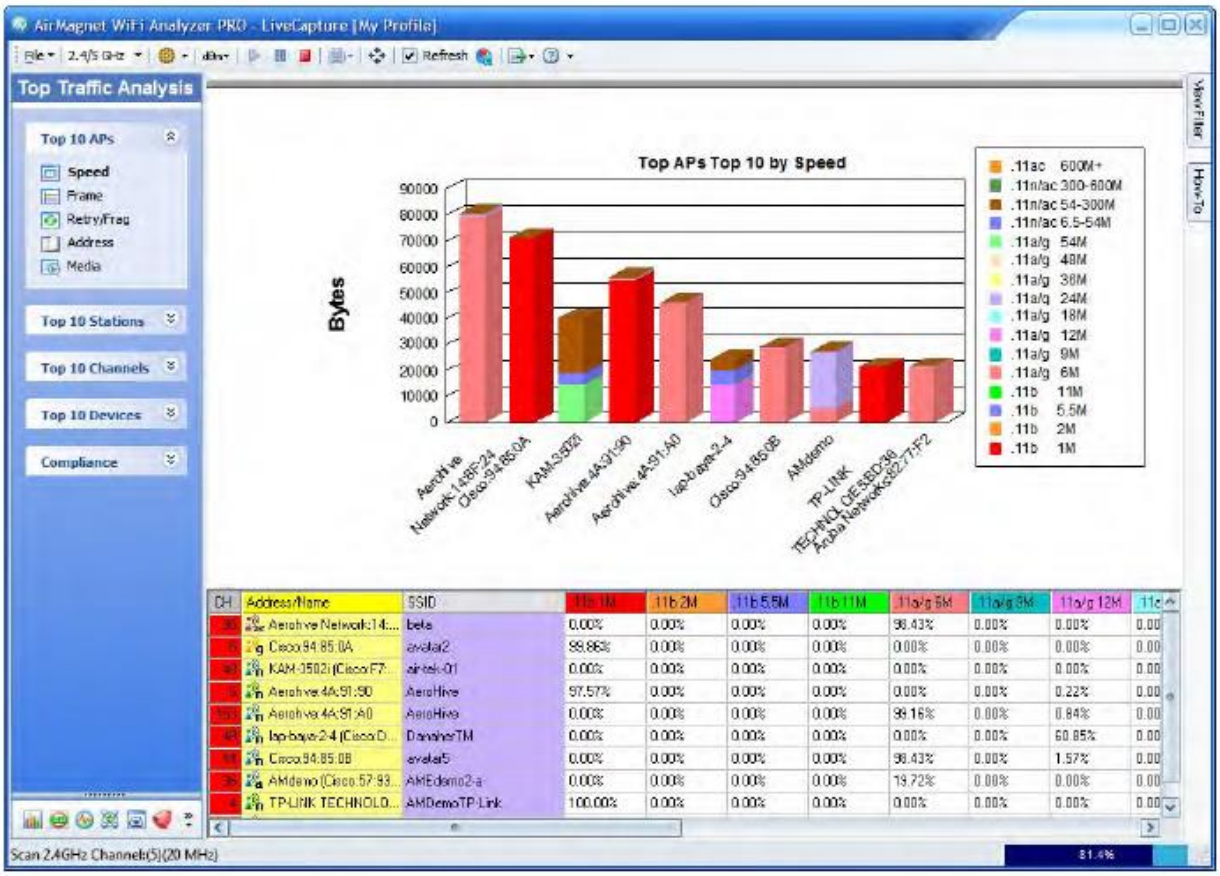
Экран Top Traffic Analysis (Анализ трафика по максимальным показателям)

Об экране Top Traffic Analysis (Анализ трафика по максимальным показателям)

Экран Top Traffic Analysis (Анализ трафика по максимальным показателям) позволяет просматривать и анализировать (в виде диаграмм) различные типы данных, захваченных на вашей сети. Чтобы перейти на экран анализа трафика по максимальным показателям, щелкните кнопкой мыши на 

на панели навигации. На приведенном ниже рисунке показан экран анализа трафика по максимальным показателям анализатора WiFi.

Примечание: Если работа ведется с разрешением экрана 800 x 600, появится разворачивающееся меню, которое позволит увеличивать масштаб отображаемых диаграмм. При использовании функции масштабирования рекомендуется убрать метку из поля Refresh (Обновить).



Меню и инструменты экрана Top Traffic Analysis (Анализ трафика по максимальным показателям)

Большая часть опций меню и инструментов на экране Top Traffic Analysis (Анализ трафика по максимальным показателям) описана в разделе «Часто используемые меню и инструменты». На рисунке ниже показана панель меню, отображаемая на экране Top Traffic Analysis.

Следующие опции меню или инструменты имеются только на экране Top Traffic Analysis:

Меню/Инструмент	Описание
	Если в этом поле установлена метка (поле выбрано), данные на экране обновляются с частотой, установленной в диалоговом окне Options (Опции). Смотрите ниже.
	Примечание: Если в данном поле стоит метка, экран Top Traffic Analysis обновляется через установленные интервалы времени, что может вызвать эффект мерцания на экране. Чтобы предотвратить это, уберите метку из этого поля.
	Позволяет открыть диалоговое окно Graph Options (Опции графика), в котором для графика можно настроить следующие параметры:  • Top devices sorted by (Сортировка устройств по) (байтам, кадрам, байтам в секунду или кадрам в секунду) • Update graph every (Обновлять график каждые) <5, 10, 15, 20 или 30> секунд. • Export file (Экспортировать файл) (необходимо либо принять имя файла по умолчанию, либо заменить его собственным уникальным именем)
	Примечание: Для настройки параметров графика сделайте нужные записи или выбор в диалоговом окне и нажмите кнопку OK.

Панель данных экрана Top Traffic Analysis (Анализ трафика по максимальным показателям)

В правой части экрана Top Traffic Analysis отображаются данные в соответствии с выбранной слева опцией. По умолчанию при открытии на экране отображаются 10 самых активных точек доступа, отсортированных по скорости передачи данных (Top 10 APs > Speed). Чтобы выбрать для отображения любую другую опцию, щелкните на ней кнопкой мыши.
Обычно для просмотра диаграммы, ориентированной на устройства, нужно выбрать категорию Top 10, а затем тип данных. После этого на экране отобразятся 10 наиболее активных устройств в выбранной категории. Однако если необходимо посмотреть наиболее активные устройства в определенных SSID или на определенных каналах, воспользуйтесь вкладкой View Filter (Фильтр просмотра) у правой кромки экрана для выбора только тех идентификаторов SSID или каналов, которые вам интересны. В этом случае можно выбрать 10 устройств в определенных SSID или на определенных каналах.

Примечание: Для любого варианта в категории Top 10 количество отображаемых на графике устройств зависит от фактического количества устройств, которые активны в сетях SSID или на каналах.

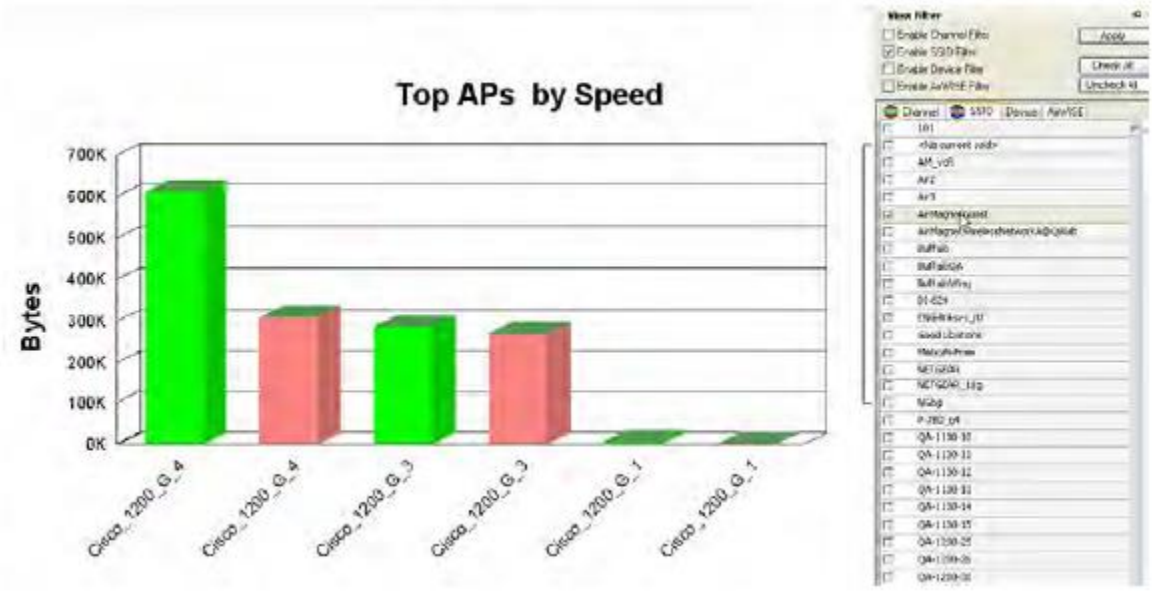
Например, если на канале обнаружено только пять устройств, то на графике будет отображаться пять устройств, даже если выбран вариант из категорий Top 10 APs (10 наиболее активных точек доступа), Top 10 Stations (10 наиболее активных станций) или Top 10 Devices (10 наиболее активных устройств).
Примечание: Если щелкнуть кнопкой мыши на любом устройстве в таблице устройств, график позволит перейти прямо на экран Infrastructure (Инфраструктура), на котором отображаются подробные данные, относящиеся к этому устройству. Название устройства будет автоматически выделено в списке устройств в левой части экрана.

Просмотр диаграмм устройств

По умолчанию при открытии экрана Top Traffic Analysis выбираются все каналы и SSID. На экране можно графически отображать 10 наиболее активных устройств в различных категориях. В разделе Compliance (Соответствие требованиям) ниже показаны различные диаграммы соответствия, дающие подробную информацию о том, насколько хорошо ваша сеть соответствует нормативным стандартам безопасности.

Каждую категорию Top 10 затем можно разделить по типу данных, как показано в разворачивающемся списке Data Type под заголовком каждого раздела.

Обычно для просмотра диаграммы устройства нужно выбрать категорию Top 10, а затем тип данных. После этого на экране отобразятся 10 наиболее активных устройств в выбранной категории. Однако если необходимо посмотреть наиболее активные устройства в определенных SSID или на определенных каналах, воспользуйтесь вкладкой View Filter (Фильтр просмотра) для выбора только тех идентификаторов SSID или каналов, которые вам интересны. В этом случае диаграмма сможет по-прежнему отображать данные до 10 устройств, но фактическое количество отображаемых устройств будет зависеть от количества устройств, которые активны в сетях SSID или на каналах.
На следующем рисунке показана диаграмма только для шести устройств с одним SSID.

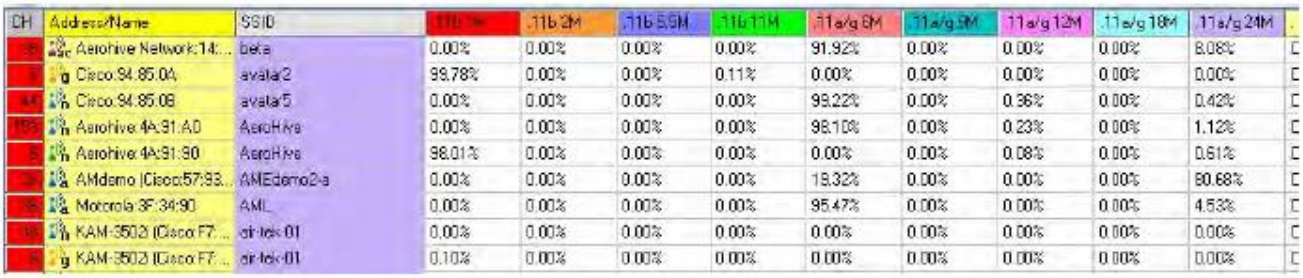


Экспортирование данных диаграммы

Для экспортирования данных текущей диаграммы можно щелкнуть кнопкой мыши на  (Экспортирование данных) в верхней части экрана диаграмм и выбрать Export Top Traffic Analysis (Экспортировать анализ максимального трафика). На экране появится сообщение с подтверждением того, что экспортирование выполнено успешно.

Табличное отображение данных диаграммы

Под графиком находится таблица с разбивкой по выбранному типу данных для 10 наиболее активных устройств.



CH	Address/Name	SSID	[illegible]	.11b 2M	.11b 5.5M	.11b 11M	.11a/g 6M	.11a/g 9M	.11a/g 12M	.11a/g 18M	.11a/g 24M	.
[illegible]	Aerohive Network:14:...	beta	0.00%	0.00%	0.00%	0.00%	91.92%	0.00%	0.00%	0.00%	8.08%	D
[illegible]	Cisco:94:85:0A	avatar2	99.78%	0.00%	0.00%	0.11%	0.00%	0.00%	0.00%	0.00%	0.00%	D
[illegible]	Cisco:94:85:08	avatar5	0.00%	0.00%	0.00%	0.00%	99.22%	0.00%	0.36%	0.00%	0.42%	D
[illegible]	Aerohive 4A:91:A0	AeroHive	0.00%	0.00%	0.00%	0.00%	98.10%	0.00%	0.23%	0.00%	1.12%	D
[illegible]	Aerohive 4A:91:90	AeroHive	98.01%	0.00%	0.00%	0.00%	0.00%	0.00%	0.08%	0.00%	0.61%	D
[illegible]	AMdemo (Cisco:57:93...	AMEdemo2-a	0.00%	0.00%	0.00%	0.00%	19.32%	0.00%	0.00%	0.00%	80.68%	D
[illegible]	Motorola:3F:34:90	AML	0.00%	0.00%	0.00%	0.00%	95.47%	0.00%	0.00%	0.00%	4.53%	D
[illegible]	KAM-3502 (Cisco:F7:...	air-tek-01	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	D
[illegible]	KAM-3502 (Cisco:F7:...	air-tek-01	0.10%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	D

Эта таблица дополняет информацию, отображаемую на диаграмме, и помогает лучше ее понять.

Таблица расширяется динамически. К каждой таблице скорости по мере того, как обнаруживаются данные для определенной скорости, динамически добавляются дополнительные столбцы. После добавления столбец остается в таблице до тех пор, пока продолжается захват данных, даже если данные с такой скоростью могут больше не обнаруживаться.

Примечание. Если на графике показаны 10 самых активных каналов, щелкните кнопкой мыши в таблице, чтобы открыть экран Channel (Канал).

Соответствие требованиям

FISMA (Федеральный закон об управлении информационной безопасностью) обязывает такие федеральные агентства, как Министерство здравоохранения и социальных служб, FCC (Федеральная комиссия по связи) и FTC (Федеральная торговая комиссия), разработать, документально оформить и реализовать программу информационной безопасности для обеспечения безопасности информации и информационных систем, которые поддерживают операции и оборудование этих агентств. Сюда включена информация и информационные системы, предоставляемые агентству другим агентством или подрядчиком.

Закон FISMA распространяется на следующее:

- BASEL II: Базельское соглашение по капиталу (Basel II) позволяет еще больше согласовать подход банков и банковских регуляторов к управлению рисками. Оно предназначено для создания минимального уровня капитала в международных банках. В отношении конкретных требований к AirMagnet, Basel II включает явные требования к капиталу для покрытия операционного риска. Операционный риск включает в себя риски в области безопасности в работе с беспроводными сетями. Соглашение Basel II является результатом развития Базельского соглашения Basel I. Они оба были разработаны Базельским комитетом по банковскому надзору (далее «комитет»). Комитет состоит из органов банковского надзора и центральных банков Группы десяти стран (G10) . К странам G10 относятся: Бельгия, Канада, Франция, Германия, Италия, Япония, Люксембург, Нидерланды, Испания, Швеция, Швейцария, Великобритания и Соединенные Штаты. Международные банки могут использовать продукты AirMagnet и отчеты о соответствии (Compliance Reports™) для выявления и смягчения операционных рисков при использовании беспроводных сетей.
- DOD 8100.2: Директива министерства обороны США (МО) за номером 8100.2 (далее «директива») объединяет основные разделы стратегии в отношении использования коммерческих беспроводных устройств, услуг и технологий в МО. Ее цель состоит в защите сетей МО от уязвимостей, присущих беспроводным сетям, что делает безопасность обязательным предварительным условием для развертывания и использования коммерческих беспроводных технологий в МО.
- EU-CRD: Директива Европейского союза о требованиях к капиталу (European Union Capital Requirements Directive), более известная как CAD3 (Capital Adequacy Directive – директива о достаточности капитала), реализует Базельское соглашение II и вводит новые требования к капиталу для международных банков, кредитных учреждений и инвестиционных компаний в ЕС. Она является развитием предыдущей директивы, которая реализовывала требования к капиталу, входившие в Базельское соглашение I. Отчеты об уровне соответствия для системы AirMagnet и для устройств определяют операционные риски в беспроводных сетях, которые могут привести к сбоям или неисправностям системы и мошенническим действиям извне.

- FISMA: Закон FISMA (Federal Information Security Management Act – федеральный закон США об управлении информационной безопасностью) обязывает такие федеральные агентства, как Министерство здравоохранения и социальных служб, FCC (Федеральная комиссия по связи) и FTC (Федеральная торговая комиссия), разработать, документально оформить и реализовать программу информационной безопасности для обеспечения безопасности информации и информационных систем, которые поддерживают операции и оборудование этих агентств. Сюда включена информация и информационные системы, предоставляемые агентству другим агентством или подрядчиком.

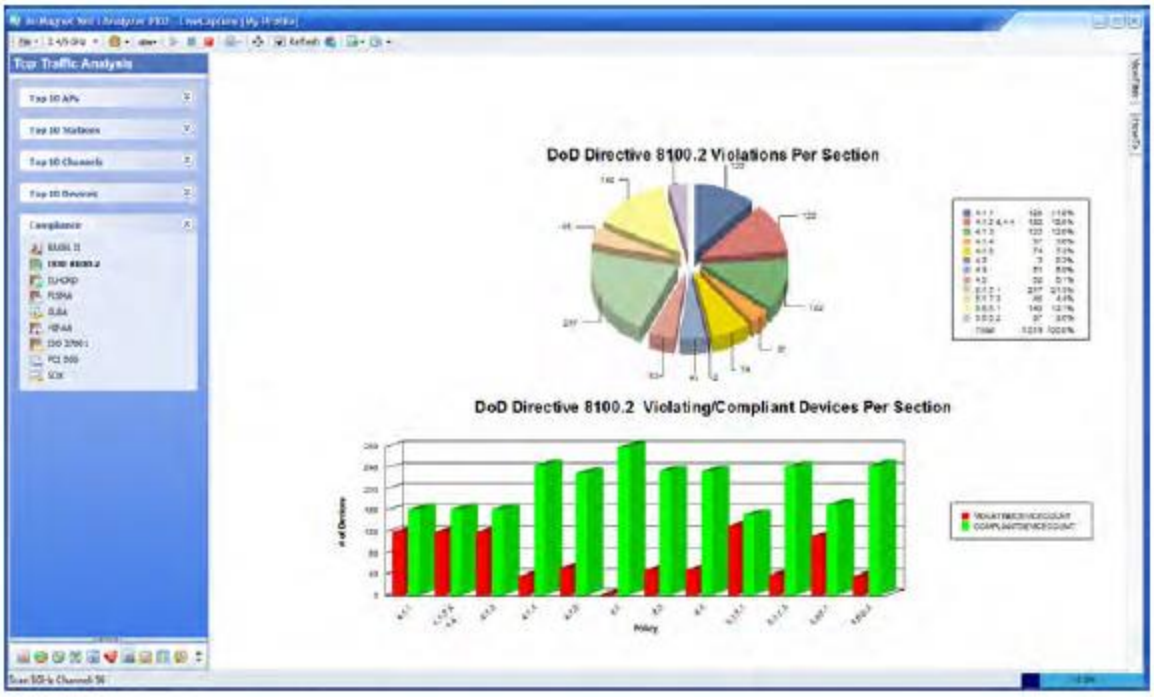
  Закон FISMA применяется к следующему:
  - Вся информация федерального правительства, за исключением информации, имеющей гриф секретности.
  - Все информационные системы, за исключением тех, которые функционируют как системы национальной безопасности.
  - Любая организация, которая является государственным органом, продает оборудование и/или программное обеспечение государственным органам или поддерживает информацию или информационные системы государственного органа.

- GLBA: Закон Грэма-Лича-Блили (GLBA), также известный как «Закон о модернизации финансовой системы 1999 года», гласит, что финансовые институты защищают безопасность и конфиденциальность личной финансовой информации своих клиентов.
- HIPPA: Закон HIPAA был принят в целях повышения эффективности национальной системы здравоохранения и содействия использованию в здравоохранении EDI (Electronic Data Interchange – электронный обмен данными). Для этого HHS (Department of Health and Human Services – министерство здравоохранения и социальных услуг) были выпущены правила защиты конфиденциальности и безопасности PHI (Protected Health Information – закрытая медицинская информация). Под PHI понимается любая медицинская информация, которая идентифицирует человека и относится к его или ее физическому или психическому здоровью.
- ISO 27001: Стандарт ISO/IEC 27001:2005 (далее ISO 27001) является международным стандартом, предназначенным для организаций любого размера и типа (государственных и негосударственных). В базе международный стандарт следует использовать в качестве модели для построения системы менеджмента информационной безопасности (Information Security Management System - ISMS). ISMS является частью организационной системы, которая управляет сетями и системами. Она основывается на рисках бизнеса и направлена на «создание, внедрение, эксплуатацию, мониторинг, обзор, поддержку и улучшение информационной безопасности». Выходя за пределы модели, организации могут получить сертификацию ISO 27001 у независимых аудиторов. Сертификация способна продемонстрировать стремление организаций к обеспечению безопасности и помочь завоевать доверие партнеров и клиентов. Также ее можно использовать в качестве доказательства соответствия законодательным требованиям, хотя сама по себе она не будет удовлетворять требованиям законодательства. Такие независимые аудиторы, как ISOQAR и LRQA (Lloyd's Registered Quality Assurance), удостоверяют соответствие организации стандарту ISO 27001. Обратите внимание, что аудиторов ISO 27001 регулируют Американское национальное бюро аккредитации (ANAB) и Служба аккредитации Соединенного Королевства. Система AirMagnet Enterprise удовлетворяет требованиям стандартов ISO 27001 и 17799 для беспроводных сетей и устройств с отчетами о соответствии на уровне системы, стратегии работы и конкретных устройств. Благодаря использованию модели ISO 27001 Plan-Do-Check-Act, решения AirMagnet способны помочь организации спланировать, проверить и действовать в направлении улучшения ISMS.
- PCI DSS: Стандарт PCI DSS (Payment Card Industry Data Security Standard – стандарт защиты информации в индустрии платежных карт) был разработан Visa и MasterCard для предотвращения кражи личных данных и мошенничества с кредитными картами. Соблюдение этого стандарта обязательно для пользователей Visa и MasterCard, поставщиков услуг, торговых компаний и тех, кто добровольно входит в другие ассоциации платежных карт, такие как American Express и Discover Card, в качестве условия для участия. Участвующие предприятия должны соответствовать 12 требованиям «лучших методов организации работы», предъявляемым к проводным и беспроводным сетям, и периодически проверять их соответствие.
- SOX: Закон Сарбейнса-Оксли (SOX), также известный как «Закон о реформе учета и отчетности в открытых компаниях и защите интересов инвесторов» был принят Конгрессом США в 2002 году как всеобъемлющее законодательство по реформированию бухгалтерского учета, раскрытия финансовой информации и корпоративного управления публичных компаний.

Примечание: Рекомендуется прочитать заявление об отказе от ответственности при использовании графиков или отчетов о сетевом соответствии приложения WiFi Analyzer.

Просмотр диаграмм соответствия

Для отображения диаграммы соответствия:
Выберите диаграмму соответствия, которую хотите отобразить, в разделе Compliance (Соответствие) на левой панели.



Отказ от ответственности

Графики и отчеты AirMagnet Basel II, DoD 8100.2, EU-CRD, FISMA, GLBA, HIPAA, ISO 27001, PCI DSS и Sarbanes Oxley Compliance обеспечивают соответствие инфраструктуры безопасности законодательству в сфере финансовых услуг, здравоохранения, общественного учета и государственного управления. В отчетах о соблюдении политики (Policy Compliance Reports) особое внимание уделяется безопасности беспроводной сети; они направлены на то, чтобы помочь сетевым администраторам в документировании их стратегии безопасности и реагировании на угрозы и инциденты в соответствии с индустриальной практикой и правительственными постановлениями.

В отчетах о соблюдении политики (AirMagnet Policy Compliance Reports) предоставляется информация о законе; отчеты предназначены для того, чтобы помочь пользователям удовлетворять требования правительственных постановлений. Однако эта информация не является юридической консультацией. Компания AirMagnet прилагает все усилия, чтобы содержащаяся в отчетах о соблюдении политики информация была точной и полезной. Если пользователю необходима юридическая консультация по тому, толкуется и внедряется ли данное программное обеспечение в полном соответствии отраслевым требованиям, компания AirMagnet, Inc рекомендует проконсультироваться с юристом.

Информация, содержащаяся в отчетах о соблюдении политик, предоставляется в соответствии с условиями лицензионного соглашения («лицензии»). Отчеты о соблюдении политики не создают обязательных деловых, юридических или профессиональных взаимоотношений между пользователями и компанией AirMagnet, Inc. Так как ведение бизнеса, технологии и законодательство в разных регионах отличаются, полное соблюдение правил будет зависеть от конкретных обстоятельств.

Top 10 APs (10 ведущих точек доступа)

Опции построения диаграммы в группе Top 10 APs (10 ведущих точек доступа) позволяют отобразить 10 ведущих точек доступа в сети в следующих категориях:

- Speed (Скорость) – На экране отображается 10 ведущих точек доступа по скорости передачи данных (то есть 1M, 2M, 5M и т.д.).

- Frame (Кадр) - На гистограмме отображается 10 ведущих точек доступа по типу кадра (то есть CRC, данные, управление и/или менеджмент).
- Retry/Frag (Повторные попытки/фрагментация) – Отображается 10 ведущих точек доступа по общему количеству кадров, повторным попыткам передачи и фрагментированным кадрам.
- Address (Адрес) – Отображается 10 ведущих точек доступа по типу адреса (то есть, широковещательный, многоадресный и/или одноадресный).
- Media (Среда) – Отображается 10 ведущих точек доступа по протоколу 802.11 (то есть 802.11a, b, g, n, ac).

Top 10 Channels (10 ведущих каналов)

Опции построения диаграммы в группе Top 10 Channels (10 ведущих каналов) позволяют отобразить 10 ведущих каналов в сети в следующих категориях:

- Speed (Скорость) – На экране отображается 10 ведущих каналов по скорости передачи данных (то есть 1M, 2M, 5M и т.д.).
- Frame (Кадр) - На гистограмме отображается 10 ведущих каналов по типу кадра (то есть CRC, данные, управление и/или менеджмент).
- Retry/Frag (Повторные попытки/фрагментация) – Отображается 10 ведущих каналов по общему количеству кадров, повторным попыткам передачи и фрагментированным кадрам.
- Address (Адрес) – Отображается 10 ведущих каналов по типу адреса (то есть, широковещательный, многоадресный и/или одноадресный).
- Media (Среда) – Отображается 10 ведущих каналов по протоколу 802.11 (то есть 802.11a, b, g, n, ac).

Top 10 Devices (10 ведущих устройств)

Опции построения диаграммы в группе Top 10 Devices (10 ведущих устройств) позволяют отобразить 10 ведущих устройств (включая точки доступа и станции) в сети в следующих категориях:

- Speed (Скорость) – На гистограмме отображается 10 ведущих устройств по скорости передачи данных (то есть 1M, 2M, 5M и т.д.).
- Frame (Кадр) - На гистограмме отображается 10 ведущих устройств по типу кадра (то есть CRC, данные, управление и/или менеджмент).
- Retry/Frag (Повторные попытки/фрагментация) – Отображается 10 ведущих устройств по общему количеству кадров, повторным попыткам передачи и фрагментированным кадрам.
- Address (Адрес) – Отображается 10 ведущих устройств по типу адреса (то есть, широковещательный, многоадресный и/или одноадресный).
- Media (Среда) – Отображается 10 ведущих устройств по протоколу 802.11 (то есть 802.11a, b, g, n, ac).

Top 10 Stations (10 ведущих станций)

Опции построения диаграммы в группе Top 10 Stations (10 ведущих станций) позволяют отобразить 10 ведущих станций в сети в следующих категориях:

- Speed (Скорость) – На экране отображается 10 ведущих станций по скорости передачи данных (то есть 1M, 2M, 5M и т.д.).
- Frame (Кадр) - Отображается 10 ведущих станций по типу кадра (то есть CRC, данные, управление и/или менеджмент).
- Retry/Frag (Повторные попытки/фрагментация) – Отображается 10 ведущих станций по общему количеству кадров, повторным попыткам передачи и фрагментированным кадрам.
- Address (Адрес) – Отображается 10 ведущих станций по типу адреса (то есть, широковещательный, многоадресный и/или одноадресный).
- Media (Среда) – Отображается 10 ведущих станций по протоколу 802.11 (то есть 802.11a, b, g, n, ac).

Просмотр отчетов о соответствии

Данные о соответствии также доступны в отчетах о соответствии. Обратитесь к разделу «Об экране Reports (Отчеты).

Отказ от ответственности для отчетов о соответствии

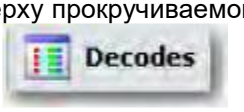
Отчеты AirMagnet DoD 8100.2, GLBA, HIPAA, Sarbanes Oxley и PCI DSS Compliance обеспечивают соответствие инфраструктуры безопасности законодательству в сфере финансовых услуг, здравоохранения, общественного учета и государственного управления. В отчетах о соблюдении политики (Policy Compliance Reports) особое внимание уделяется безопасности беспроводной сети; они направлены на то, чтобы помочь сетевым администраторам в документировании их стратегии безопасности и реагировании на угрозы и инциденты в соответствии с индустриальной практикой и правительственными постановлениями.

В отчетах о соблюдении политики (AirMagnet Policy Compliance Reports) предоставляется информация о законе; отчеты предназначены для того, чтобы помочь пользователям удовлетворять требования правительственных постановлений. Однако эта информация не является юридической консультацией. Компания AirMagnet прилагает все усилия, чтобы содержащаяся в отчетах о соблюдении политики информация была точной и полезной. Если пользователю необходима юридическая консультация по тому, толкуется и внедряется ли данное программное обеспечение в полном соответствии отраслевым требованиям, компания AirMagnet, Inc рекомендует проконсультироваться с юристом.

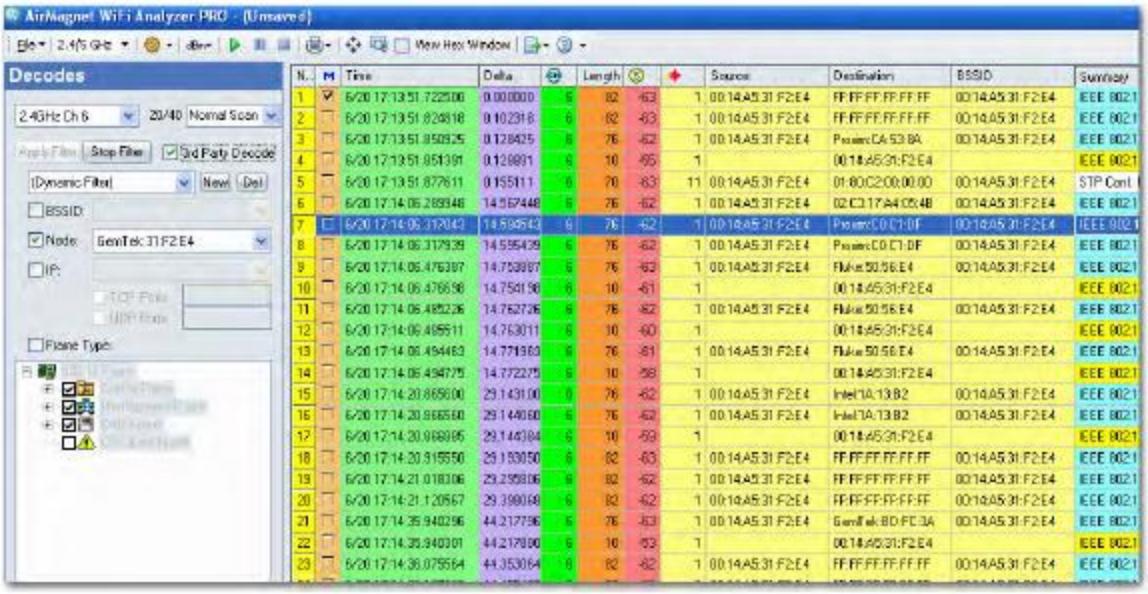
Информация, содержащаяся в отчетах о соблюдении политик, предоставляется в соответствии с условиями лицензионного соглашения («лицензии»). Отчеты о соблюдении политики не создают обязательных деловых, юридических или профессиональных взаимоотношений между пользователями и компанией AirMagnet, Inc. Так как ведение бизнеса, технологии и законодательство в разных регионах отличаются, полное соблюдение правил будет зависеть от конкретных обстоятельств.

Экран Decodes (Декодирование)

Об экране Decodes (Декодирование)

По умолчанию на экране Decodes (Декодирование) в реальном времени по мере захвата отображаются все кадры пакетов. Пакеты отображаются в последовательности захвата, причем последние всегда отображаются вверху прокручиваемого списка. Чтобы открыть экран Decodes (Декодирование), щелкнув кнопкой мыши на 

на панели навигации. Экран Decodes (Декодирование) приложения AirMagnet WiFi Analyzer показан на рисунке ниже.

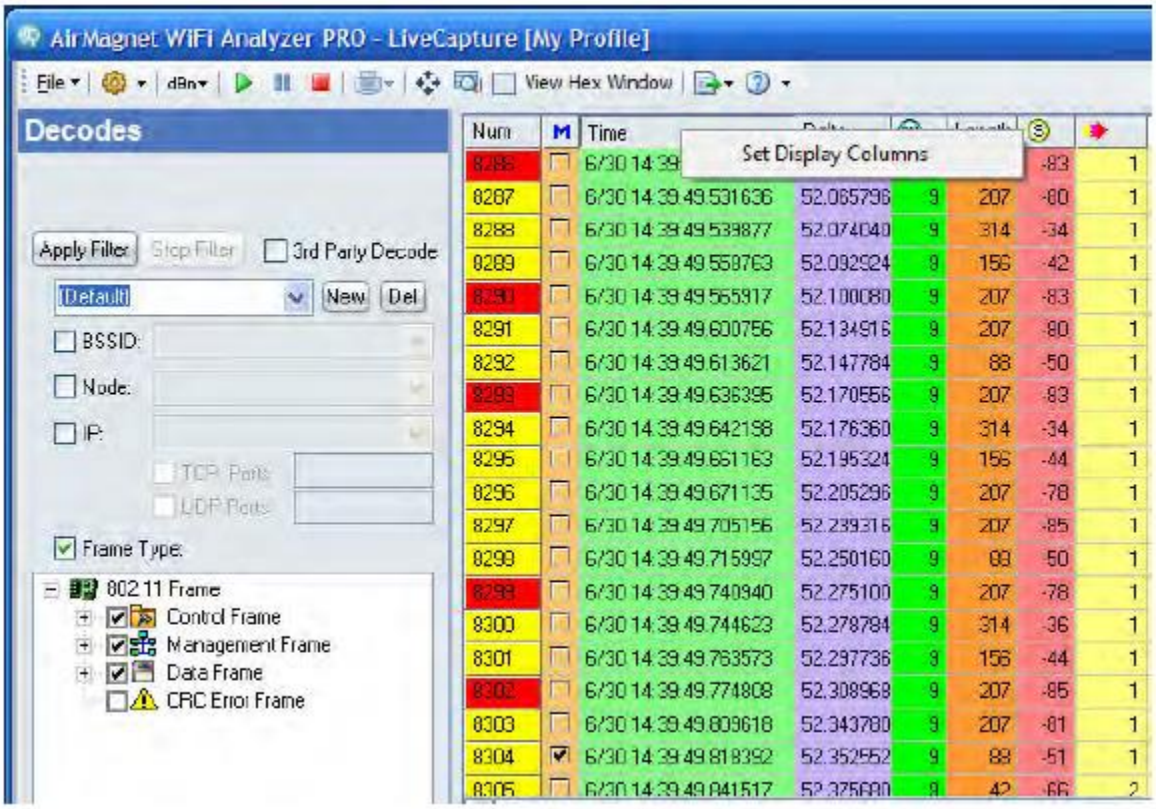


Добавление/удаление столбцов

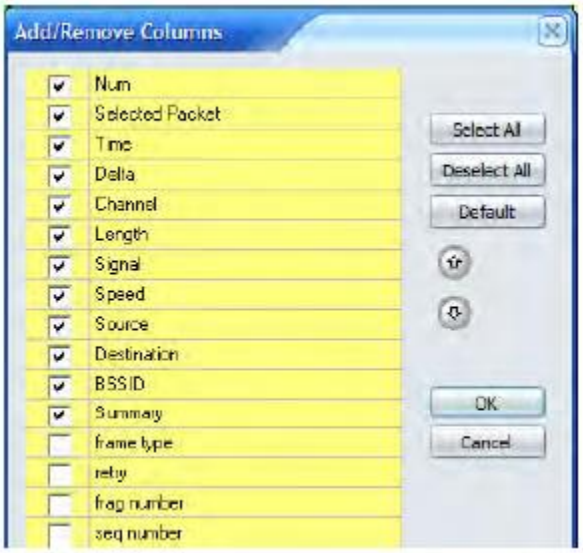
Диалоговое окно Add/Remove Columns (Добавить/удалить столбцы) можно использовать для выбора столбцов, которые будут отображаться в таблице декодирования.

Для добавления или удаления столбцов в таблице декодирования (Decodes):

1. Щелкните правой кнопкой мыши на заголовке столбца в таблице Decodes (Декодирование), чтобы открыть всплывающее окно Set Display Columns (Настроить отображаемые столбцы). Выберите Set Display Columns. Смотрите рисунок ниже.



2. Для выбора отображаемых столбцов используйте поля для установки меток. Нажмите кнопку OK. Смотрите рисунок ниже.



В этом разделе рассматриваются следующие темы, касающиеся экрана Decodes (Декодирование):

- Поля информации о пакете
- Настройка фильтров пакетов
- Создание нового фильтра
- Использование настраиваемого фильтра
- Выполнение декодирования пакетов
- Поиск пакетов на экране Decodes (Декодирование)

Приложение AirMagnet WiFi Analyzer имеет два разных режима захвата в реальном времени: обычный режим и режим захвата на диск (Capture-to-Disk).

- Обычный режим захвата: Максимальный размер памяти захвата составляет 64 Мбайта, и захваченные данные сохраняются в файле формата .amc. Данный режим хорошо подходит для сбора небольшого количества данных сетевого трафика.
- Режим захвата на диск (Capture-to-Disk): Данный режим позволяет приложению передавать захваченные данные трафика Wi-Fi на жесткий диск компьютера одновременно с захватом данных в реальном времени. Благодаря этой функции объем захватываемых данных больше не ограничивается размером буфера захвата.

По умолчанию при запуске приложения функция Capture-to-Disk (Захват на диск) отключена. Она включается вручную пользователем (используйте File > Configure > Profile > Capture to Disk > File Size (Файл > Настроить > Профиль > Захват на диск > Размер файла)). После включения данный режим сохраняется, пока не будет достигнут максимальный размер файла захвата (Maximum Capture File Size). На изображении выше показан экран Decodes (Декодирование) в режиме Capture-to-Disk (Захват на диск). В строке состояния в правом нижнем углу экрана отображается размер дискового пространства, выделенного для сохранения захвата (то есть 512 Мбайт), а также процент или объем использованного дискового пространства. Иконка диска указывает, что приложение находится в режиме захвата на диск (Capture-to-Disk).
Кнопка Pause Live capture (Приостановить захват в реальном времени) на панели инструментов доступна только в режиме Capture-to-Disk (Захват на диск). Она неактивна, когда приложение находится в обычном режиме захвата (то есть .amc).
По умолчанию кнопка Apply Filter (Применить фильтр) в верхней левой части экрана отключена (неактивна). Она становится доступной только после внесения изменений на экране. В этом случае для применения изменений, внесенных в фильтры, необходимо нажать эту кнопку.

Поля информации о пакете

На экране Decodes (Декодирование) предоставлены различные данные о каждом захваченном пакете. Каждая часть информации отображается в отдельном столбце, описанном в таблице ниже.

Столбец	Описание
No (Номер)	Последовательность захваченных пакетов, отображаемая только тогда, когда захват пакетов остановлен.
M	Поставьте метку в этом поле, чтобы начать отсчет кадров с выбранного пакета. В столбце Delta для этого пакета будет установлен 0, и будет вестись соответствующая нумерация для будущих пакетов. Отображается, только когда захват пакетов остановлен.
Time (Время)	Время получения пакета. Отображается, только когда захват остановлен.
Frame Gap (Интервал кадров)	Промежуток времени между двумя кадрами.
Delta	Время, прошедшее между каждым пакетом. Отображается, только когда захват остановлен.
CH	Канал.
S	Мощность сигнала.
Length (Длина)	Длина кадра.
Speed (Скорость)	Скорость, с которой передавался пакет.
Source (Источник)	Исходный узел.
Destination (Место назначения)	Узел, являющийся местом назначения.
BSSID	BSSID (Идентификатор основных наборов служб) источника.
Summary (Сводка)	Сводка пакета данных.

Настройка фильтров пакетов

Приложение AirMagnet WiFi Analyzer по умолчанию поставляется с заводскими настройками фильтра. Чтобы ограничить захват пакетов определенным каналом, SSID, точкой доступа, станцией или типом кадра, можно также настроить свои собственные фильтры. Имейте в виду, что использование фильтров не является обязательным. Они предназначены для того, чтобы помочь сконцентрировать анализ на определенном канале, SSID, узле, IP-адресе или типе кадров, если это необходимо. Кроме того, фильтры можно использовать по отдельности или в любой комбинации, которую позволяет приложение.

В левой части экрана Decodes (Декодирование) содержатся параметры фильтрации данных, отображаемых на экране. По умолчанию кнопка Apply Filter (Применить фильтр) отключена (выделена серым цветом) и не будет доступна, пока не будут внесены изменения в настройки фильтра. После внесения изменений в настройки фильтра для их применения необходимо нажать Apply Filter (Применить фильтр).

Примечание: Панель Filter (Фильтр) в левой части экрана Decodes (Декодирование) является зеркальным отображением вкладки Filter (Фильтр) экрана Configure (Настройка). Однако фильтры на странице Decodes (Декодирование) влияют только на данные, отображаемые на этой странице, тогда как главный фильтр применяется ко всем страницам. Если необходимо настроить главный фильтр для глобальной работы, щелкните кнопкой мыши на  и выберите вкладку Filter (Фильтр), чтобы открыть экран конфигурации фильтра. Дополнительная информация приводится в разделе «Настройка фильтров данных».

Создание пользовательских фильтров

Приложение AirMagnet WiFi Analyzer позволяет пользователям создавать собственные фильтры, используя настройки фильтрации по своему выбору. После создания такие настраиваемые фильтры автоматически сохраняются в приложении для использования в будущем, и доступны до тех пор, пока не будут удалены.

Для создания собственного фильтра:

1. Щелкните кнопкой мыши на New (Создать) и замените [New Filter] уникальным именем фильтра.
   - Чтобы сосредоточиться на конкретном идентификаторе SSID, отметьте поле SSID и выберите идентификатор в меню List (Список).
   - Чтобы сосредоточиться на конкретном узле в сети, отметьте поле Node (Узел) и выберите MAC-адрес этого узла в меню List (Список).
   - Чтобы сосредоточиться на конкретном IP-адресе, отметьте поле IP и выберите IP-адрес в меню List (Список). Также можно указать порт TCP и/или UDP, если такая информация имеется.
2. Выберите интересующие вас кадр или кадры.

Применение фильтра

После создания фильтры остаются доступными при каждом запуске приложения. Они упрощают мониторинг трафика по каналу, идентификатору SSID, узлу или типу кадра.

Для применения фильтра:

1. Если хотите сфокусироваться на конкретном канале, выберите его.
2. Щелкните кнопкой мыши на направленной вниз стрелке и выберите нужный фильтр. Смотрите рисунок ниже.

3. Нажмите кнопку Apply Filter (Применить фильтр).

Примечание: Меню списка содержит все созданные вами фильтры. Если необходимо отключить используемый фильтр, нажмите кнопку Stop Filter (Остановить фильтр). Для удаления любого фильтра, выделите его в меню списка и нажмите Del (Удалить).

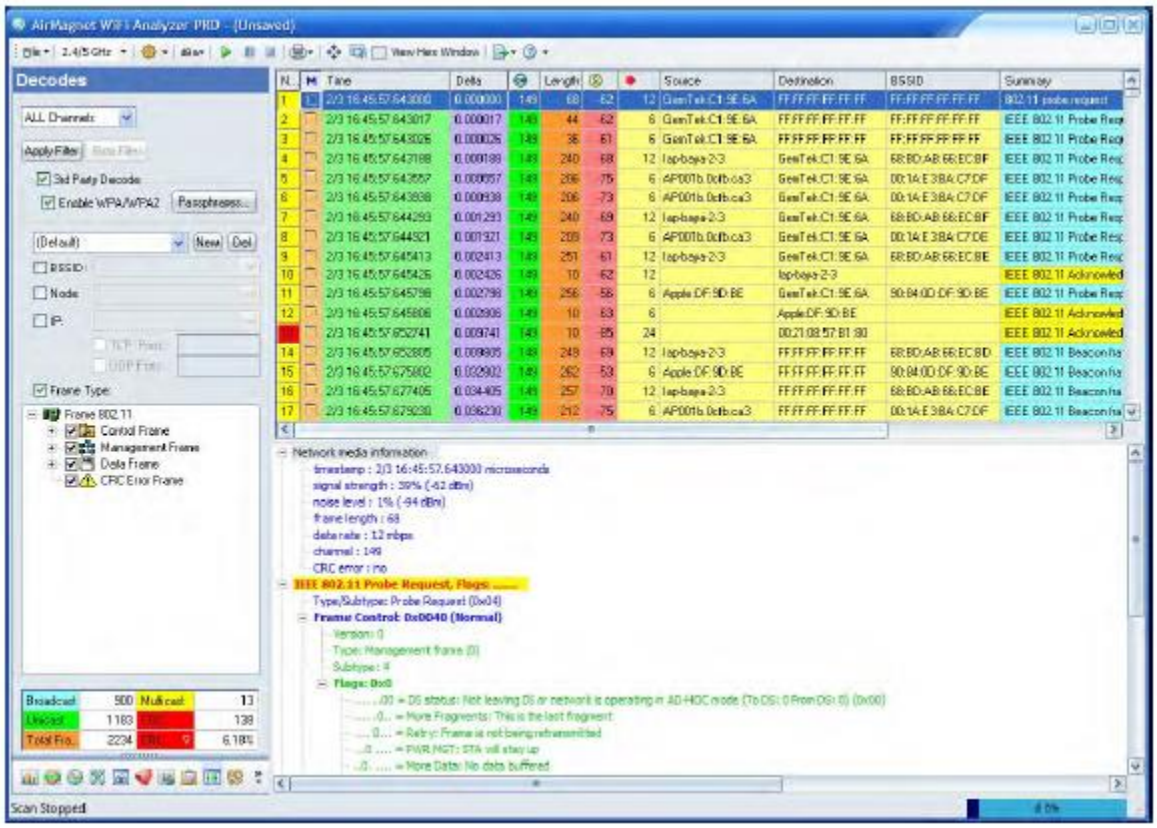
Выполнение декодирования пакетов

По умолчанию на экране Decodes (Декодирование) пакеты данных отображаются последовательно по мере их захвата (прокручиваются по принципу «первым пришел - первым ушел»). Для проведения подробного анализа пакетов необходимо остановить прокрутку экрана, чтобы получить возможность найти и внимательно рассмотреть любой пакет.

Примечание: Если во время установки продукта была установлена функция поддержки декодирования верхнего уровня (сторонние декодеры), при просмотре захваченных данных появляется возможность переключения между декодированием по умолчанию и декодером сторонних производителей. Если же во время установки приложения установка этой функции не была выбрана, ее можно установить в любое время на вкладке Filter (Фильтр) диалогового окна Configuration (Конфигурация).

На первом представленном ниже рисунке показан вид с использованием декодера стороннего производителя. На втором рисунке показан механизм декодирования по умолчанию.
При использовании декодера стороннего производителя незашифрованные данные также обеспечивают декодирование верхнего уровня.

Для более внимательного ознакомления со списком декодированных пакетов на экране остановите захват в реальном времени, нажав  (Остановить захват в реальном времени). Чтобы возобновить захват пакетов, нажмите кнопку  (Начать захват в реальном времени).



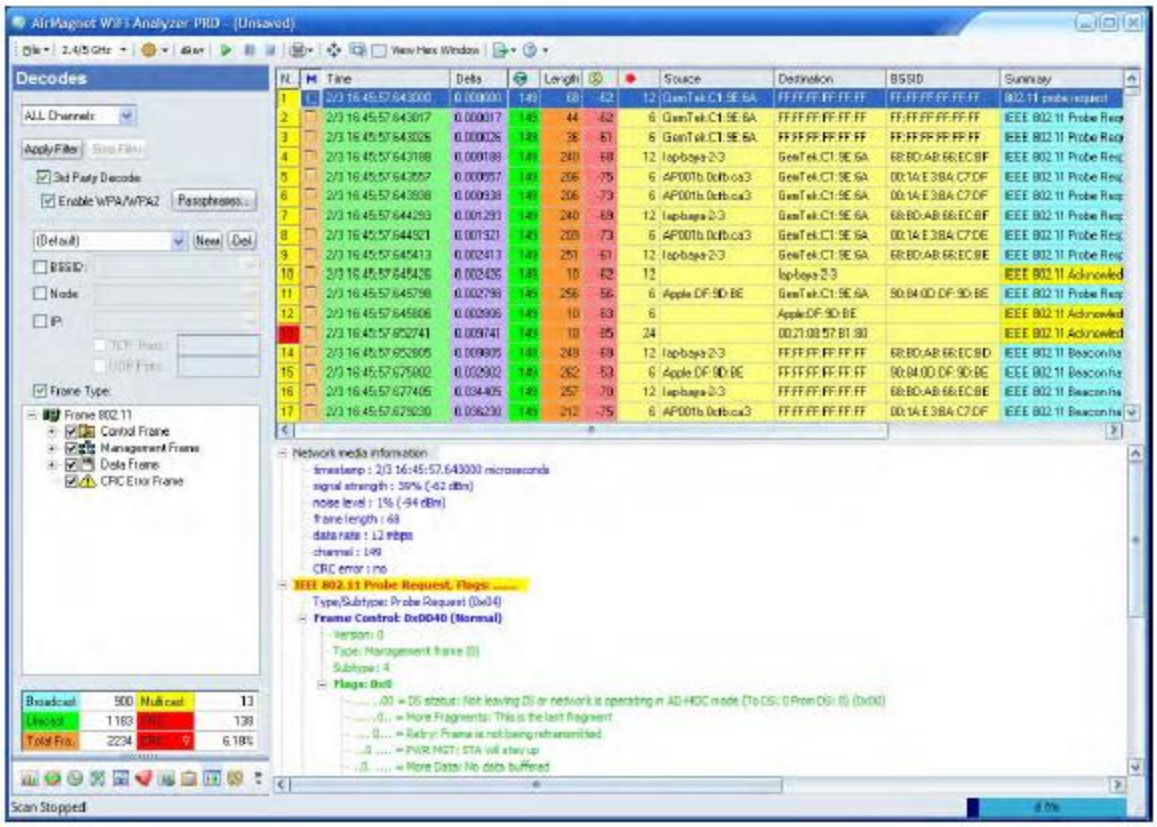
Включены декодеры сторонних производителей

Примечание: Кнопка временной остановки декодирования () доступна только в случае включения режима Capture to Disk (Захват на диск) (.amm); она не применяется в обычном режиме захвата в реальном времени (.amc). На приведенном выше изображении показан экран Decodes (Декодирование),

когда приложение находится в режиме Capture to Disk (Захват на диск). Если выбран обычный режим захвата, для декодирования захваченных пакетов следуйте приведенным ниже инструкциям.

Для выполнения декодирования пакета:

1. На панели инструментов щелкните кнопкой мыши на  . Экран Decodes (Декодирование) постепенно останавливается. Смотрите рисунок ниже.



Экран декодирования по умолчанию

2. На панели инструментов поставьте метку в поле View Hex Window (Просматривать шестнадцатеричное окно).
3. Выберите пакет на экране и просмотрите всю информацию о нем.
4. Запустите декодирование пакета, развернув все записи в нижней части экрана.
5. Повторяйте шаги 3 и 4 для анализа других интересующих вас пакетов.
6. Чтобы возобновить захват пакетов в реальном времени, нажмите  (Начать захват в реальном времени).

Примечание: Щелкните правой кнопкой мыши на дереве пакетов, чтобы выбрать параметры быстрого развертывания и свертывания дерева: Expand Subtrees (Развернуть поддеревья), Expand All (Развернуть всё), Collapse All (Свернуть всё).

Расшифровка WPA/WPA2-PSK

Расшифровку устройств, использующих шифрование WPA/WPA2-PSK, можно проводить с помощью SSID и парольной фразы для WPA/WPA2-PSK. Расшифровка WPA-PSK поддерживается только в режиме CTD (захват на диск).

Если пакет зашифрован, в столбце Summary (Сводка) экрана Decodes (Декодирование) будет указана фраза «encrypted data» (зашифрованные данные).
Расшифровка требует захвата целых кадров, включая четырехэтапный процесс установления связи между клиентом и точкой доступа. Помните, что при расшифровке кадров важно, чтобы сканирование было зафиксировано на канале.

Расшифровка также поддерживается для файла трассировки, который включает четырехэтапный процесс установления связи и предоставляет правильный SSID с парольной фразой.

1. На экране Decodes (Декодирование) поставьте метку в поле 3rd Party Decodes (Сторонние декодеры). (Если эта функция недоступна, ее необходимо установить. Обратитесь к вкладке Filter (Фильтр) диалогового окна Configuration (Конфигурация).)
2. Поставьте метку в поле Enable WPA/WPA2 (Включить WPA/WPA2).
3. Щелкните кнопкой мыши на Passphrase (Парольная фраза).

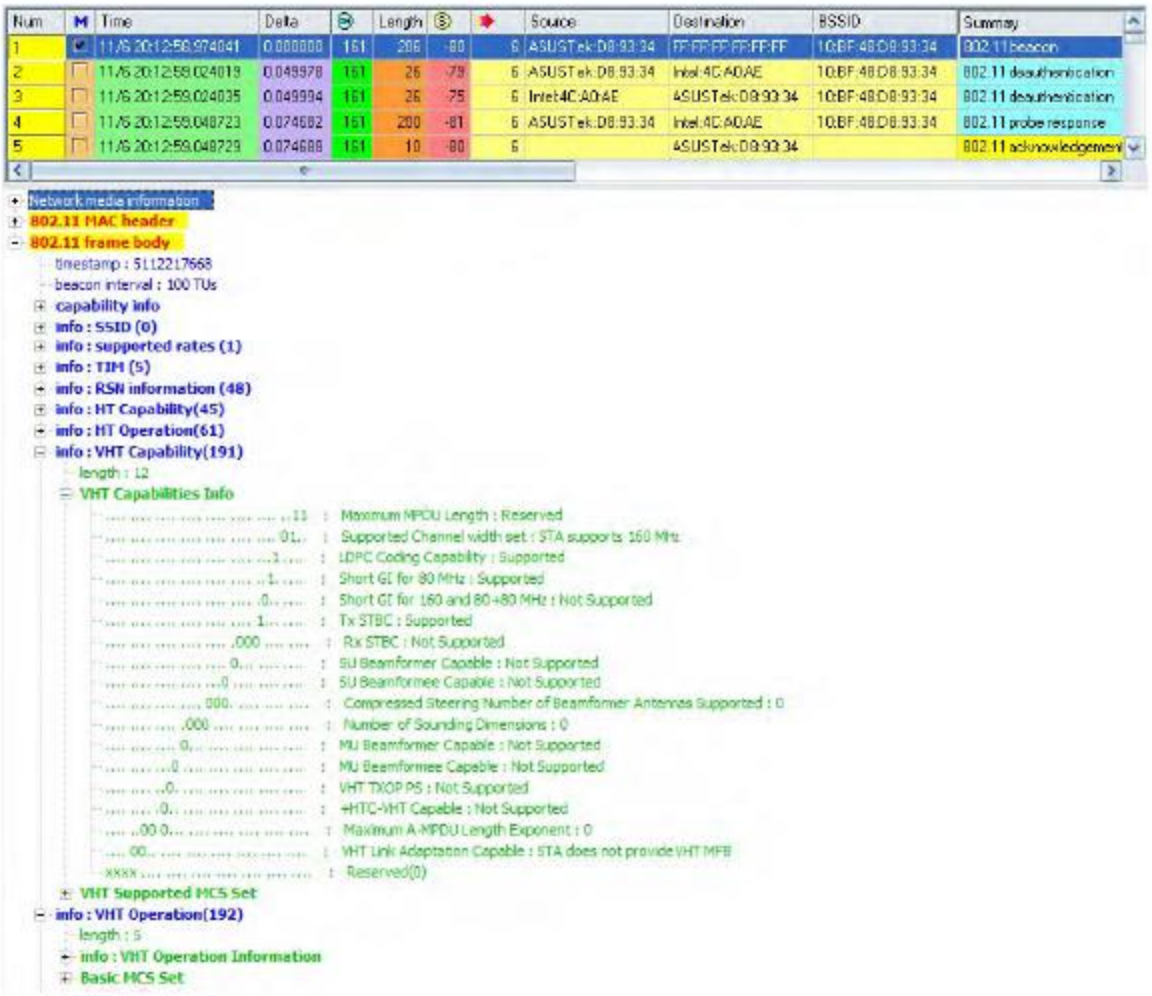
4. Нажмите New (Создать). Введите SSID и парольную фразу (Passphrase). Нажмите кнопку OK.
5. Чтобы закрыть диалоговое окно, нажмите кнопку OK.

После создания ключ дешифрования можно отредактировать (Edit) и удалить (Delete), используя соответствующие параметры в диалоговом окне Decryption Key Management (Управление ключами дешифрования).
Созданный набор ключей дешифрования можно экспортировать для использования в другом экземпляре приложения AirMagnet WiFi Analyzer.

1. Откройте диалоговое окно Decryption Key Management (Управление ключами дешифрования). Создайте один или несколько ключей дешифрования.
2. Нажмите Export (Экспортировать) и сохраните настройки ключа дешифрования.
3. Откройте экземпляр приложения AirMagnet WiFi Analyzer. Перейдите на экран Decodes (Декодирование).
4. Откройте диалоговое окно Decryption Key Management (Управление ключами дешифрования).
5. Нажмите кнопку навигации Import (Импортировать) и перейдите в папку, где был сохранен файл настроек (Preferences).
6. Выберите файл с именем Preferences.
7. Нажмите Open (Открыть).
8. Нажмите Import (Импортировать).

Декодирование 802.11ac

В приведенном ниже примере на экране Decodes (Декодирование) показаны кадры управления 802.11ac в режиме VHT Capability (Совместимость с очень высокой пропускной способностью).



Поиск пакетов на экране Decodes (Декодирование)

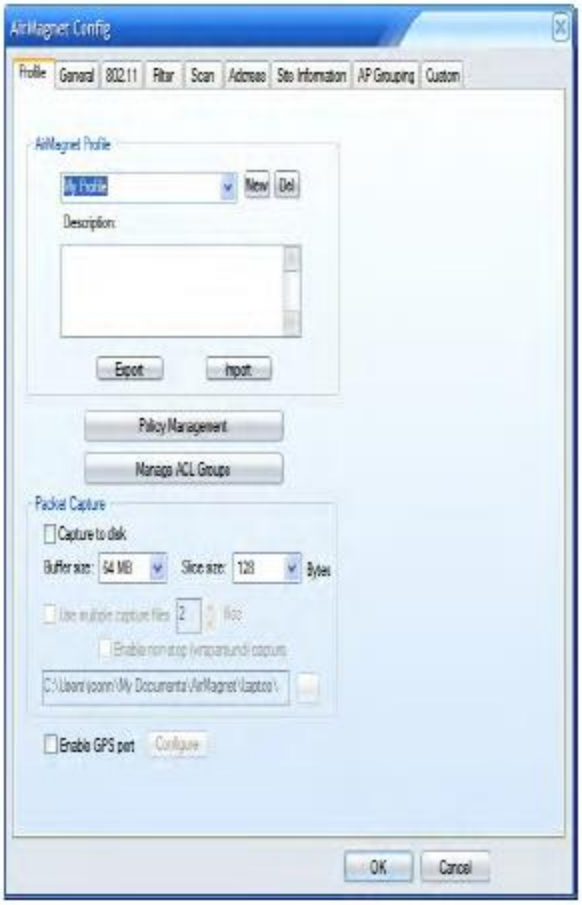
При декодировании пакетов быстро найти конкретный пакет на экране можно с помощью  (Найти на этом экране), если известна основная информация об искомом пакете.

Чтобы найти конкретный пакет:

1. На экране Decodes (Декодирование) щелкните кнопкой мыши на  (Остановить захват в реальном времени).
2. На панели меню щелкните кнопкой мыши на  . Откроется диалоговое окно Find (Найти). Смотрите рисунок ниже.

3. Сделайте необходимые записи и выбор, и нажмите кнопку Find (Найти).

Захват и сохранение большого объема данных



Для захвата пакетных данных на диск можно выбрать любой из двух методов:
Capture to disk (Захват на диск): Поставьте метку в этом поле, чтобы захватить и сохранить файл максимального размера, выбранного в разворачивающемся списке Buffer size (Размер буфера). Также можно выбрать размер Byte slice (Вырезка в байтах) в разворачивающемся списке Slice size (Размер вырезки). Захват данных останавливается по достижении размера буфера.
Когда буфер будет заполнен, появится диалоговое окно, в котором предоставлена возможность сохранения файла на диск.

Non-stop Capture (Непрерывный захват): Если также установить метку в поле Non-stop Capture (Непрерывный захват), при достижении настроенного размера буфера (Buffer size) данные будут автоматически сохраняться в папке, указанной в текстовом поле сохранения файла. Именем файла будет дата/время. В этот момент автоматически начнется новый сбор данных. Процесс будет продолжаться до

тех пор, пока не будет достигнуто установленное максимальное выделенное дисковое пространство (HDD) (по умолчанию 10 Гбайт). Максимальный размер выделенного дискового пространства может быть равным всему доступному пространству на диске.

Для захвата и сохранения большого объема данных:
1. На панели инструментов выберите File > Configure… (Файл > Настроить).
2. Откройте вкладку Profile (Профиль).
3. Установите метку в поле Capture to Disk (Захват на диск). Для непрерывного захвата также поставьте метку в поле Non-Stop Capture.
4. Выберите размер файла (File Size) и размер вырезки (Slice Size).
5. Если используется режим Non-stop Capture (Непрерывный захват), установите максимальное выделенное дисковое пространство (HDD).
6. Используйте кнопку обзора справа от текстового поля сохранения файла, чтобы указать место для его сохранения.
7. Нажмите кнопку ОК.

Декодирование пакетов одновременно с захватом в реальном времени

Эта функция позволяет выполнять подробное декодирование пакетов в режиме захвата в реальном времени, не выходя из приложения. В отличие от обычной операции декодирования, которая полностью останавливает захват в реальном времени и приводит к пропуску некоторого сетевого трафика, эта функция позволяет выполнять декодирование, не пропуская никаких данных, проходящих через сеть.

Для выполнения декодирования пакетов одновременно с захватом в реальном времени:
1. На панели инструментов выберите File > Configure > Profile (Файл > Настроить > Профиль).
2. Поставьте метку в поле Capture to Disk (Захват на диск), выберите размер файла (File size) и размер вырезки (Slice size), и нажмите кнопку ОК.

Примечание: После включения функции Capture to Disk (Захват на диск) в строке состояния в правом нижнем углу будет отображаться общий объем выделенного дискового пространства, а также объем или процент использованного пространства.

3. На экране Decodes (Декодирование) щелкните кнопкой мыши на  (Приостановить декодирование).
4. Убедитесь, что в поле View Hex Window стоит метка.
5. Выполните декодирование, используя ту же процедуру, которая описана в разделе «Выполнение декодирования пакетов».
6. По завершении щелкните кнопкой мыши на  (Начать захват в реальном времени), чтобы возобновить захват в реальном времени.

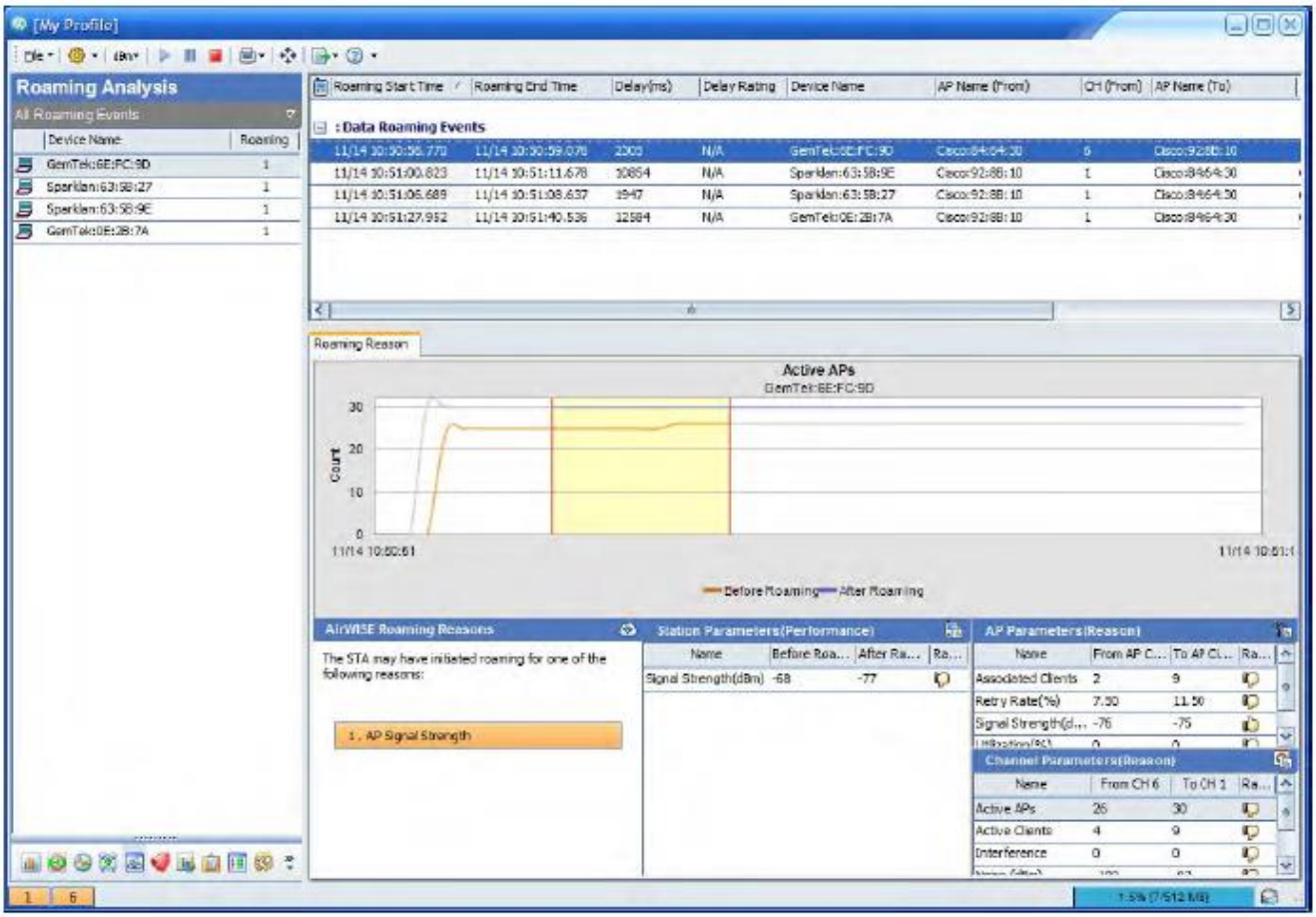
Примечание: При щелчке кнопкой мыши на иконке «Приостановить декодирование» автоматически выделяется пакет в нижней части списка захвата пакетов. Это указывает, что данный пакет захвачен в этот момент времени. Поскольку захват в реальном времени все еще продолжается даже во время декодирования, медленное перемещение полосы прокрутки справа укажет на захват новых пакетов.

Экран Roaming (Роуминг)

Об экране Roaming Analysis (Анализ роуминга)

На экране Roaming Analysis (Анализ роуминга) показаны все устройства, для которых было обнаружено переключение с одной точки доступа на другую. На экране также представлена подробная информация обо всех обнаруженных событиях роуминга, связанных с каждым устройством.

Чтобы перейти на экран Roaming Analysis (Анализ роуминга), щелкните на  на панели навигации. На рисунке показан экран анализа роуминга Wi-Fi.



В этом разделе рассматриваются следующие темы, касающиеся экрана Roaming Analysis (Анализ роуминга):

- Список устройств
- Подробности анализа роуминга

Список устройств

На расположенной слева панели списка устройств по умолчанию отображаются все события роуминга (All Roaming Events). Обычно это является отправной точкой для любого анализа роуминга. Чтобы отфильтровать список устройств, выберите подходящий вариант в разворачивающемся списке.

Начните анализ с выбора устройства в списке.

Как показано на рисунке выше, информация представлена в форме таблицы, которая содержит дополнительные сведения о каждом устройстве.

Столбец	Описание
(Иконка)	В первом столбце просто отображается иконка, соответствующая типу обнаруженного устройства.
Device Name/Channel (Имя устройства/канал)	По умолчанию в этом столбце отображается имя устройства. Если имя не было введено, то оно создается с использованием комбинации имени производителя устройства и последних шести цифр его MAC-адреса. При просмотре роуминга по каналам в этом столбце просто указывается номер канала.
Roaming (Роуминг)	Это поле позволяет быстро оценить количество случаев роуминга для данного устройства или канала. Более высокие значения могут указывать на то, что у устройства возникают проблемы с подключением, и может потребоваться дополнительный анализ, описанный в разделе «Анализ подробностей роуминга».
Roaming In/Out (Подключений/отключений в роуминге)	Эти столбцы присутствуют только при просмотре списка устройств (Device Listing) по точке доступа (AP) или каналу (Channel). Значение, указанное для параметра Roaming In, указывает общее количество раз, когда устройства в роуминге подключились к указанной точке доступа или указанному каналу. В столбце Roaming Out указано, сколько раз устройства отключились в роуминге. Большое количество переключений устройств для канала или точки доступа может указывать на недостаточное покрытие сигнала в этой области.

Примечание: Столбцы в таблице могут отличаться в зависимости от параметра просмотра, выбранного с помощью фильтра событий роуминга (Roaming Event Filter), описанного ниже.

Фильтр событий роуминга

Для облегчения оценки данных с помощью разворачивающегося фильтра, расположенного в верхней части панели, можно настроить информацию, которая будет отображаться в списке устройств.

Так как перечень отображаемых столбцов зависит от сделанного выбора, можно выполнить настройку так, чтобы отображать только требуемые данные:

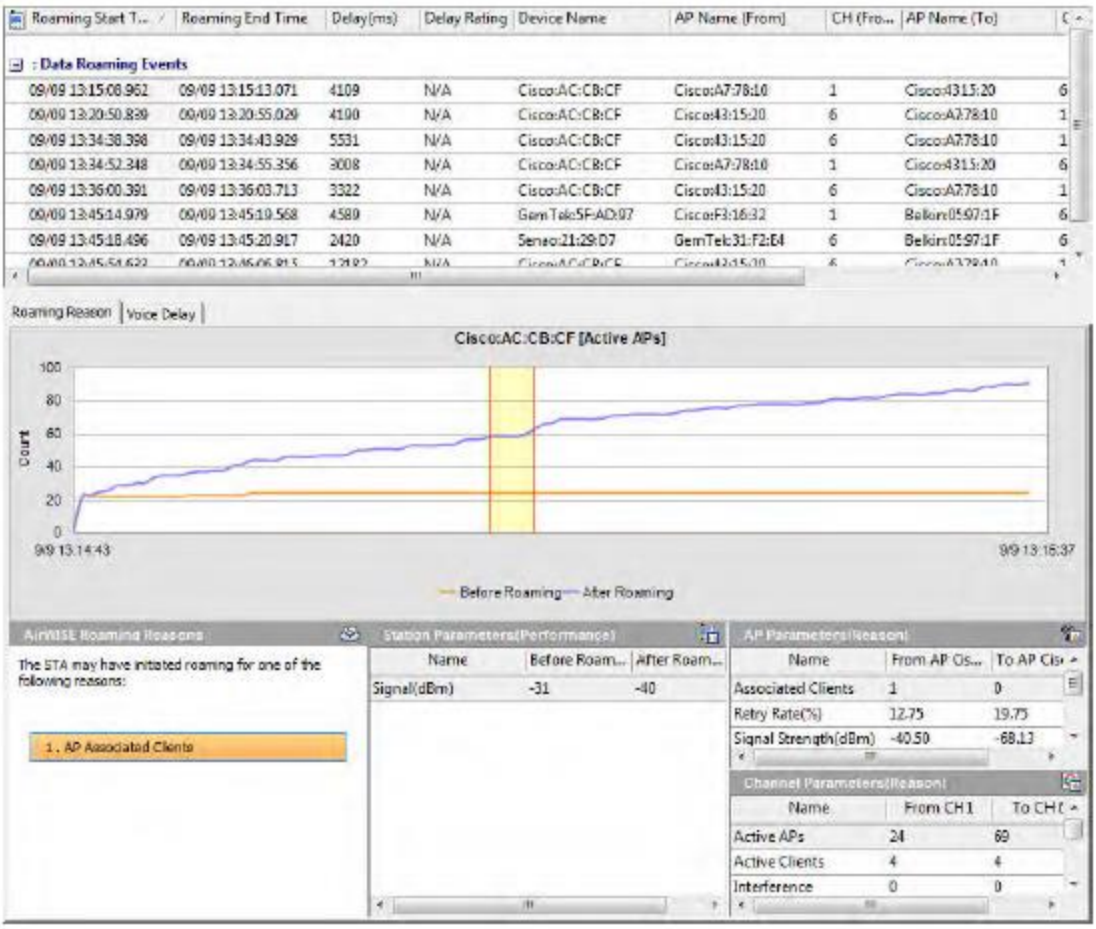
- All Roaming Events (Все события роуминга) – Вариант по умолчанию. Обеспечивает широкий обзор всех устройств, находящихся в роуминге, и количества обнаруженных случаев роуминга. В этот список могут входить как стандартные беспроводные станции, так и телефоны VoFi.
- List by Station (Список по станциям) – При выборе этой опции отображаются только беспроводные станции, то есть телефоны отфильтровываются. Эту опцию удобно использовать в средах, где голосовой трафик уже считается достаточным для потребностей присутствующих пользователей, но трафик данных при этом, похоже, страдает.
- List by Phones (Список по телефонам) – В отличие от списка по станциям данный фильтр игнорирует случаи роуминга данных и позволяет пользователю полностью сосредоточиться на роуминге телефона VoFi.
- List by AP (Список по точкам доступа) – В этом списке перечислены все точки доступа, участвовавшие в роуминге (к которым или от которых переходили устройства), а также количество случаев, обнаруженных для каждой из них. Точки доступа, сталкивающиеся с большим объемом роуминга, могут быть перегружены, что указывает на необходимость дополнительной инфраструктуры в этом регионе.
- List by Channel (Список по каналам) – Последний фильтр позволяет пользователю просматривать случаи роуминга с разделением на отдельные обнаруженные каналы. Как и в случае выбора списка по точкам доступа, пользователь может просматривать количество случаев роуминга, как на каждый канал, так и от него; большое количество перемещений с канала может указывать на то, что в этом конкретном частотном диапазоне присутствует слишком много помех.

Круговая диаграмма роуминга

В нижней части списка устройств представлена круговая диаграмма Voice Delay (Задержка голоса) для обнаруженных случаев роуминга VoFi. Это значение времени, которое проходит между последним пакетом, переданным через начальную точку доступа, и первым пакетом, переданным через новую точку доступа (то есть точку доступа, на которую переключился телефон в роуминге). Значение Voice Delay является главным показателем качества разговора по VoFi; более высокая задержка может вызвать задержки при обмене данными между двумя телефонами и, в конечном итоге, привести к обрыву соединения.

Анализ сведений о роуминге

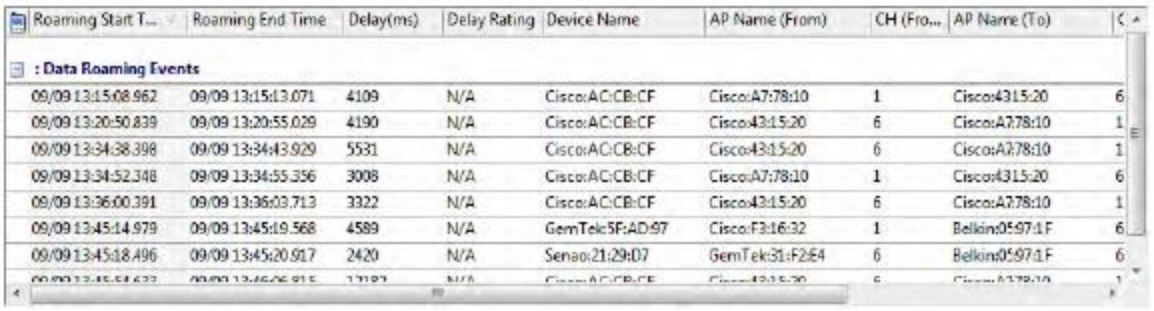
Большую часть экрана Roaming Analysis (Анализ роуминга) занимает панель Roaming Details (Сведения о роуминге), на которой предоставлены подробные данные на основе выбора, сделанного в списке устройств. После совершения выбора на левой панели (щелчком кнопкой мыши на нужном устройстве или канале) информация в разделе Roaming Details (Сведения о роуминге) обновится, и отражает данные, относящиеся к сделанному выбору.



Из-за объема доступной информации панель сведений о роуминге разделена на три основных раздела: таблица случаев роуминга (вверху), причины роуминга (первая вкладка, выбранная снизу) и информация о задержке передачи голоса (вторая вкладка).

Таблица случаев роуминга

Верхняя часть панели содержит таблицу, в которой отображаются все случаи роуминга, обнаруженные для выбранного устройства. В зависимости от устройства эти случаи могут быть либо событиями роуминга данных (Data Roaming Events), либо событиями роуминга голоса (Voice Roaming Events). Чтобы просмотреть данные роуминга для определенного события, щелкните кнопкой мыши на желаемой записи в таблице, и другие части экрана обновятся соответствующим образом.



Roaming Start T...	Roaming End Time	Delay(ms)	Delay Rating	Device Name	AP Name (From)	CH (Fro...	AP Name (To)	C
: Data Roaming Events								
09/09 13:15:08.962	09/09 13:15:13.071	4109	N/A	Cisco:AC:CB:CF	Cisco:A7:78:10	1	Cisco:43:15:20	6
09/09 13:20:50.839	09/09 13:20:55.029	4190	N/A	Cisco:AC:CB:CF	Cisco:43:15:20	6	Cisco:A7:78:10	1
09/09 13:34:38.398	09/09 13:34:43.929	5531	N/A	Cisco:AC:CB:CF	Cisco:43:15:20	6	Cisco:A7:78:10	1
09/09 13:34:52.348	09/09 13:34:55.356	3008	N/A	Cisco:AC:CB:CF	Cisco:A7:78:10	1	Cisco:43:15:20	6
09/09 13:36:00.391	09/09 13:36:03.713	3322	N/A	Cisco:AC:CB:CF	Cisco:43:15:20	6	Cisco:A7:78:10	1
09/09 13:45:14.979	09/09 13:45:19.568	4589	N/A	GemTek:5F:AD:97	Cisco:F3:16:32	1	Belkin:05:97:1F	6
09/09 13:45:18.496	09/09 13:45:20.917	2420	N/A	Senao:21:29:07	GemTek:31:F2:E4	6	Belkin:05:97:1F	6

Столбцы таблицы содержат разнообразные данные для случаев роуминга VoFi и роуминга данных, как описано в таблице ниже.

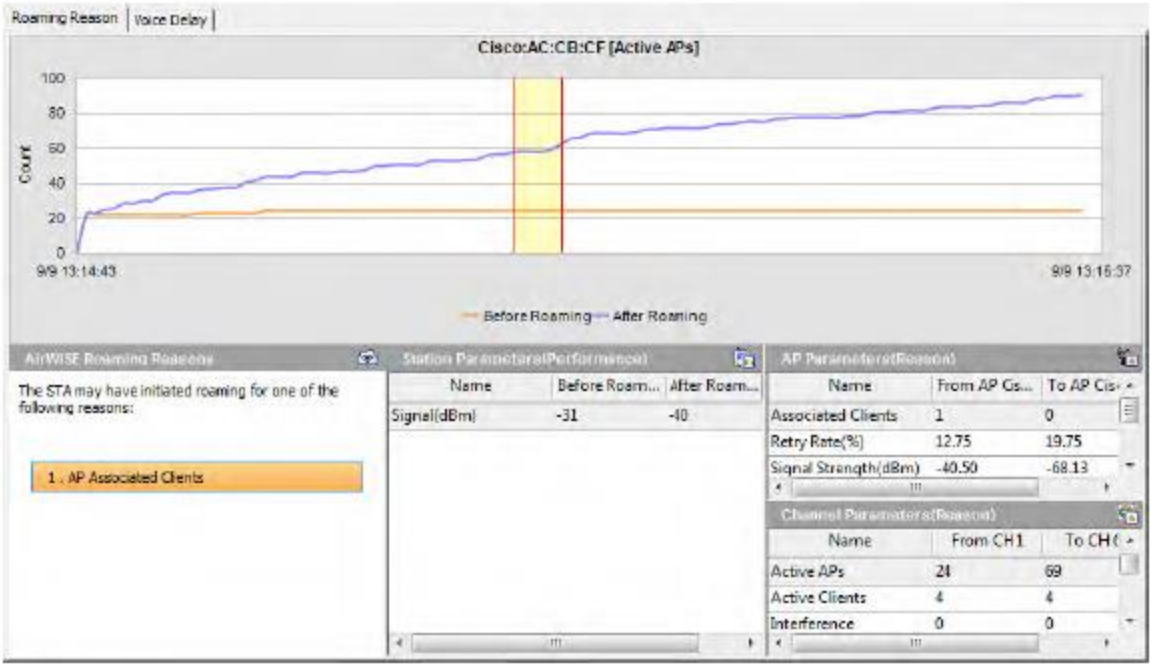
Столбец	Описание
(Иконка)	Иконки в первом столбце указывают тип устройства, связанного с каждым событием; роуминг данных обозначается значком компьютера, тогда как роуминг VoFi обозначается значком телефона.
Roaming Start/End Time (Время начала/окончания роуминга)	Время начала и завершения процесса роуминга устройством.
Delay (ms) (Задержка (мс))	Задержка, измеряемая от момента, когда последний пакет был передан на исходную точку доступа, до момента, когда первый пакет был передан на новую точку доступа.
Rating (Рейтинг)	Иконки, представленные в столбце Rating, показывают, улучшилось ли беспроводное обслуживание устройства в результате роуминга. Данный показатель рассчитывается на основе значения задержки. По умолчанию задержка более 500 мс указывает на плохой роуминг, поскольку устройству потребовалось слишком много времени, чтобы установить новое соединение, и оно могло прервать любые вызовы или передачу данных, которые обрабатывались во время роуминга.
	Примечание: Столбец Rating относится только к вызовам VoFi; для роуминга данных будет просто отображаться «N/A».
Device Name (Имя устройства)	Имя устройства в роуминге.
AP Name (From/To) (Имя точки доступа (с/на))	В этих столбцах указаны имена точек доступа, участвующих в процессе роуминга (то есть исходной точки доступа, и той, на которую подключалось устройство).
CH (From/To) (Канал (с/на))	В этих столбцах отображается исходный канал (до роуминга) и последний канал (после роуминга).
Signal (From/To) (Сигнал (с/на))	В этих столбцах отображается уровень сигнала, обнаруженный до и после роуминга.
MOS (From/To) (MOS (с/на))	В этих полях отображается оценка MOS (Средняя экспертная оценка) для соединения как до, так и после роуминга.
	Примечание: Столбцы MOS относятся только к вызовам VoFi; для данных будет просто отображаться «N/A».

Определение причины роуминга

По умолчанию при первом входе на экран Roaming Analysis (Анализ роуминга) отображается вкладка Roaming Reason (Причина роуминга). Данный выбор позволяет получить доступ к множеству разных субпанелей, которые помогут определить причину конкретного случая роуминга.

Вкладка Roaming Reason (Причина роуминга)

Выбор вкладки Roaming Reason (Причина роуминга) в нижнем левом углу экрана позволяет определить потенциальные причины для выбранного случая роуминга. Это приводит к изменениям в частях Roaming Chart (Диаграмма роуминга), Delay (Задержка) и Decodes (Декодирование) на экране.



Примечание: На панели Roaming Reasons (Причины роуминга) в нижнем левом углу экрана перечислены возможные причины возникновения роуминга. Щелчок кнопкой мыши на этих причинах настраивает диаграмму на отображение данных, которые могут помочь в диагностике роуминга.

Тип отображаемой диаграммы будет зависеть от выбора, сделанного на панелях в нижней части экрана. Как показано выше, щелчок кнопкой мыши на какой-либо из ссылок на панели Roaming Reasons (Причины роуминга) приводит к соответствующему обновлению диаграммы. Однако диаграмма также будет обновляться в зависимости от выбора, сделанного на панелях Phone Parameters (Параметры телефона), AP Parameters (Параметры точки доступа) или Channel Parameters (Параметры канала).

Примечание: При осуществлении выбора на любой из панелей параметров на диаграмме появляется стрелка, указывающая на характеристики вызова до и после роуминга.

На каждой из панелей параметров данные отображаются в трех основных столбцах:

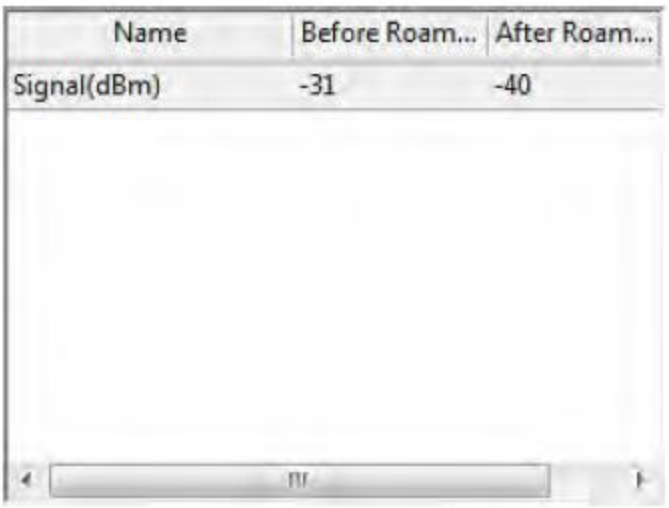
- Before Roam (Перед роумингом) – Отображаемые в первом столбце данные соответствуют вызову до роуминга.
- After Roam (После роуминга) – Во втором столбце отображаются данные, обнаруженные по завершении роуминга.
- Rating (Рейтинг) – В последнем столбце отображается значок с направленным вверх большим пальцем, если категория (например, MOS (Средняя экспертная оценка), частота повторных попыток (Retry Rate), джиттер (Jitter) и т.д.) улучшилась после роуминга. Если же в результате роуминга категория пострадала, появится значок с направленным вниз большим пальцем.

Эти данные способны помочь в выявлении проблем, влияющих на субъективные ощущения во время разговора. Например, при роуминге, показанном на рисунке выше, улучшается показатель Retry Rate

(Частота повторных попыток) и CRC Errors (Ошибки CRC) (как показано в Phone Parameters (Параметры телефона)), но джиттер (Jitter) значительно увеличился в результате роуминга. Это может указывать на то, что пользователь будет испытывать дополнительные трудности в поддержании разговора.

Device Parameters (Параметры устройства)

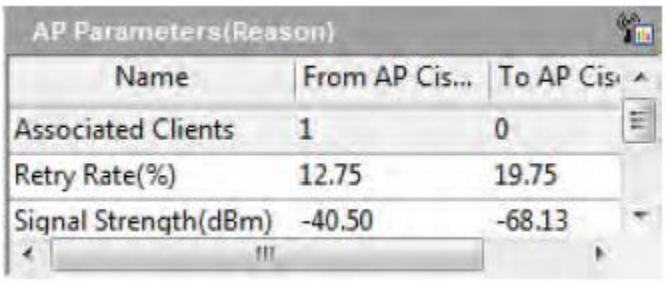
Правее панели Roaming Reasons (Причины роуминга) находится поле Device Parameters (Параметры устройства), которое зависит от типа выбранного случая роуминга. Для случаев роуминга данных отображаются частота повторных попыток, ошибки CRC и уровень сигнала как до, так и после роуминга. Для роуминга VoFi эти данные дополняются информацией MOS и Jitter.



Name	Before Roam...	After Roam...
Signal(dBm)	-31	-40

AP Parameters (Параметры точки доступа)

При устранении неисправностей, приводящих к повторяющимся случаям беспроводного роуминга, полезно определить, какой объем трафика обрабатывают точки доступа в данной области. Эту информацию предоставляет поле AP Parameters (Параметры точки доступа), указывающее количество вызовов и клиентов, обслуживаемых обеими точками доступа, которые участвуют в выбранном случае роуминга (например, исходной и конечной точками доступа).



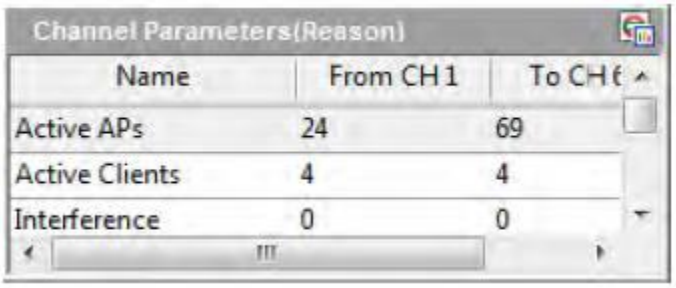
AP Parameters(Reason)

Name	From AP Cis...	To AP Cis
Associated Clients	1	0
Retry Rate(%)	12.75	19.75
Signal Strength(dBm)	-40.50	-68.13

Как показано выше, также можно посмотреть частоту повторных попыток, мощность сигнала и степень использования до и после роуминга. Эта информация может быть полезна для определения того, был ли роуминг оправданным. Если исходная точка доступа имела низкий уровень сигнала непосредственно перед роумингом, возможно, станция или телефон просто удалялись из этого региона и нуждались в поиске более близкого источника беспроводной связи.

Channel Parameters (Параметры канала)

В поле Channel Parameters (Параметры канала) представлен быстрый обзор каналов, участвующих в роуминге, который позволяет определить, не является ли основной причиной возникновения проблемы переполненный или заблокированный канал.



Определив количество точек доступа и клиентов, присутствующих на выбранном канале, можно увидеть, не было ли во время роуминга в среде слишком много активных устройств. Большое количество беспроводных клиентов может вызывать помехи, которые способны ухудшить качество связи. Точно так же высокие уровни шумов и использования могут привести к уменьшению полосы пропускания, доступной для подключения клиента.

Вкладка Voice Delay (Задержка голоса)

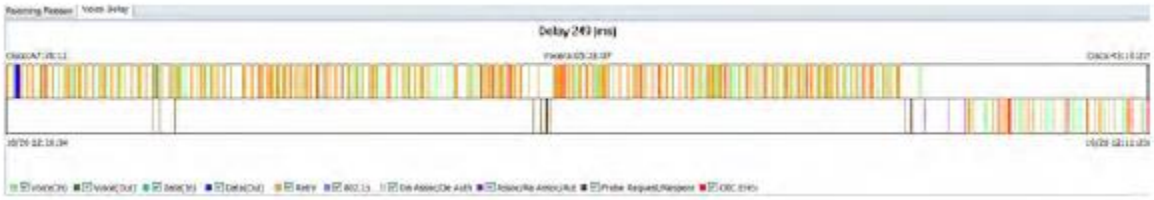
Примечание: Вкладка Voice Delay (Задержка голоса) будет доступна только в том случае, если выбран случай роуминга VoFi, поскольку приведенная на ней информация не применяется к стандартному роумингу данных.

На вкладке Voice Delay (Задержка голоса) представлен обзор всех данных, относящихся к роумингу VoFi, что идеально позволяет использовать ее для устранения неисправностей в локализованных случаях чрезмерного роуминга. В следующих разделах объясняется информация, представленная на этой вкладке.

- Диаграмма пакетов
- Анализ задержки (Delay Analysis)
- Декодирование пакетов

Диаграмма пакетов

После того, как в таблице роуминга сделан необходимый выбор, диаграмма пакетов обновится для отображения подробной диаграммы кадров, переданных и полученных во время разговора как до, так и после события роуминга.

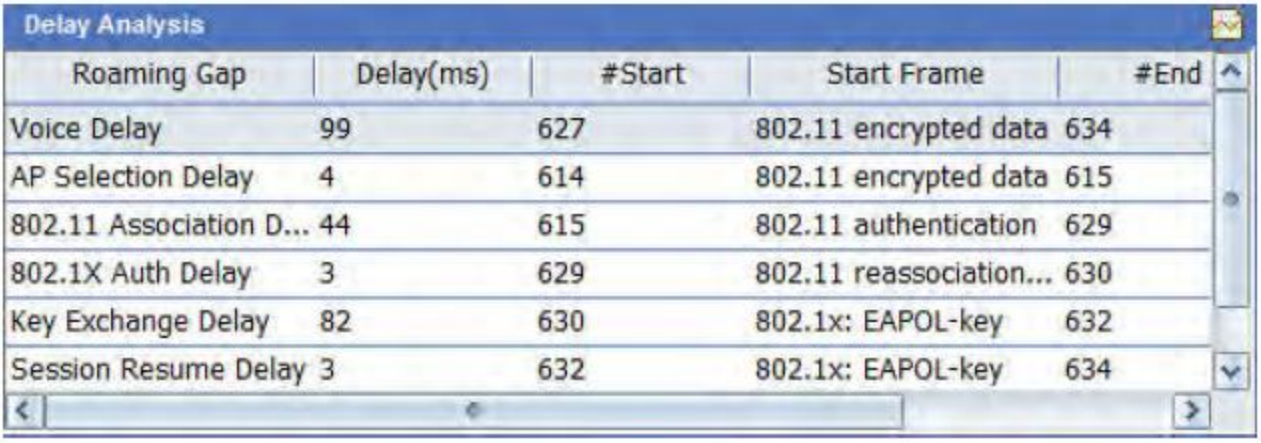


На диаграмме выбранный случай роуминга выделен красным цветом, а по обе стороны от разрыва отображаются пакеты с цветовой кодировкой. Для просмотра кадров, обнаруженных во время вызова, можно ставить или убирать метки из полей опций в цветовой легенде.

Примечание: Экран отображения потока кадров разделен на две части. Кадры, собранные до начала роуминга, отображаются в верхней части диаграммы, а кадры, собранные после роуминга, отображаются в ее нижней части.

Delay Analysis (Анализ задержки)

В разделе Delay Analysis (Анализ задержки) отображается продолжительность задержек, обнаруженных во время роуминга, включая время, затраченное на выбор новой точки доступа, подключение к ней и возобновление разговора.



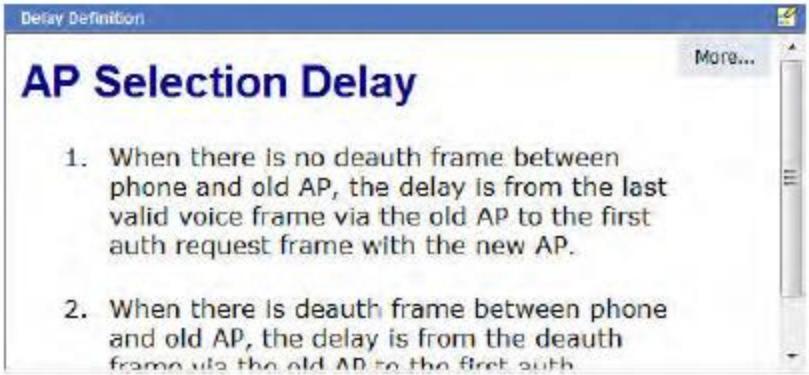
Roaming Gap	Delay(ms)	#Start	Start Frame	#End
Voice Delay	99	627	802.11 encrypted data	634
AP Selection Delay	4	614	802.11 encrypted data	615
802.11 Association D...	44	615	802.11 authentication	629
802.1X Auth Delay	3	629	802.11 reassociation...	630
Key Exchange Delay	82	630	802.1x: EAPOL-key	632
Session Resume Delay	3	632	802.1x: EAPOL-key	634

Верхняя часть панели Delay Analysis (Анализ задержки) (Voice Delay - задержка голоса) разбивает общую задержку во время роуминга на несколько (до пяти) компонентов, описанных ниже:

- AP Selection Delay (Задержка выбора точки доступа) – Время, затраченное на выбор точки доступа, которая обеспечит лучшее качество связи.
- 802.11 Association Delay (Задержка подключения 802.11) – Время, затраченное на процесс подключения к новой точке доступа.
- 802.11 Authentication Delay (Задержка аутентификации 802.1x) – Время, необходимое для аутентификации в сетях с поддержкой 802.1x.
- Key Exchange Delay (Задержка на обмен ключами) – Задержка, связанная с обменом ключами 802.1x.
- Session Resume Delay (Задержка возобновления сеанса) – Время между успешной аутентификацией и следующим переданным голосовым кадром.

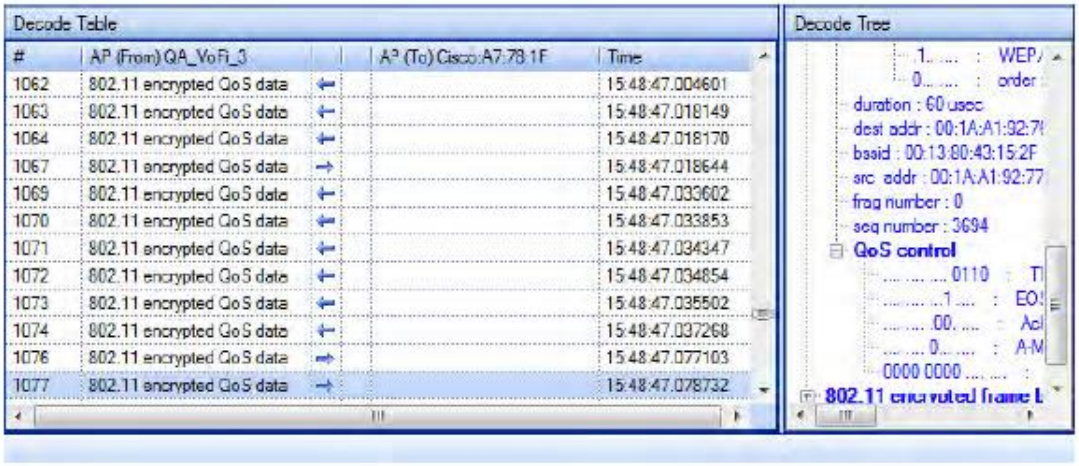
Примечание: Выбор определенной опции задержки в таблице Delay Analysis (Анализ задержки) настраивает диаграмму пакетов на отображения кадров, соответствующих сделанному выбору.

В нижней части окна отображаются дополнительные сведения о выбранной задержке. Эту информацию можно просмотреть, прокручивая при необходимости, для получения конкретных данных о том, как определяется задержка. Для получения дополнительных сведений нажмите More Info.



Для идентификации пакетов, переданных до и после события роуминга, используйте таблицу и дерево декодирования. При выборе определенного пакета его сводка отображается в дереве декодирования.

Декодирование пакетов



В таблице ниже описаны столбцы, которые составляют таблицу декодирования (Decode Table).

Поле	Описание
#	Номер кадра в транзакции роуминга.
AP (From) (Точка доступа (с))	Точка доступа, от которой отключился телефон при выполнении операции роуминга.
[Стрелки]	Стрелки указывают направление, в котором перемещается каждый кадр. Например, стрелка, указывающая вправо, означает, что кадр был отправлен с телефона на точку доступа. Стрелка, указывающая влево, означает, что кадр был передан с точки доступа на телефон.
AP (To) (Точка доступа (на))	Точка доступа, к которой телефон подключился после выполнения роуминга.
Time (Время)	Время, когда кадр был отправлен.

Несколько адаптеров

Функция нескольких адаптеров – это возможность использования нескольких адаптеров Wi-Fi для одновременного захвата трафика. Каждый адаптер «фиксируется» на одном канале на все время захвата. Это означает, что захватывается весь трафик тех каналов, на которых зафиксированы адаптеры, что позволяет проводить анализ уже после захвата. Еще одним важным преимуществом использования нескольких адаптеров является одновременный многоканальный мониторинг.

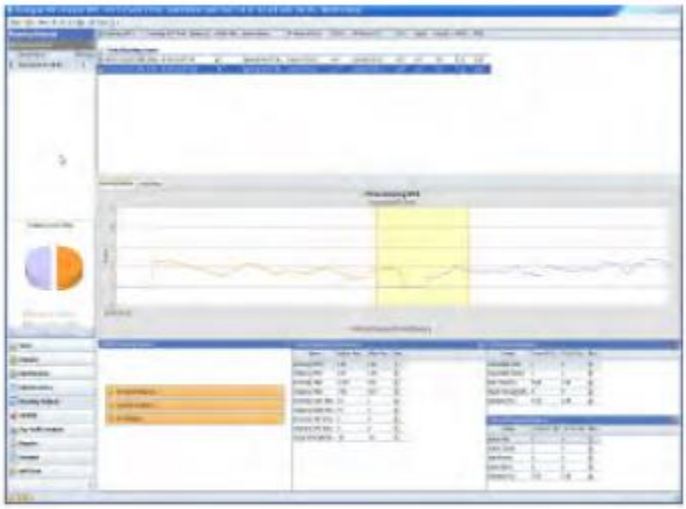
Примечания: 1) Страница Roaming Analysis (Анализ роуминга) требует использования мультиадаптеров. 2) Пакеты, захваченные от нескольких адаптеров, сохраняются как один файл.

Для использования всех преимуществ применения нескольких адаптеров разные страницы используют разные режимы визуализации данных. Смотрите таблицу случаев роуминга.
Для экранов, связанных с конкретным адаптером, на панели инструментов появляется новое меню, позволяющее указать используемый адаптер. Обратитесь к разделу «Использование нескольких беспроводных адаптеров».

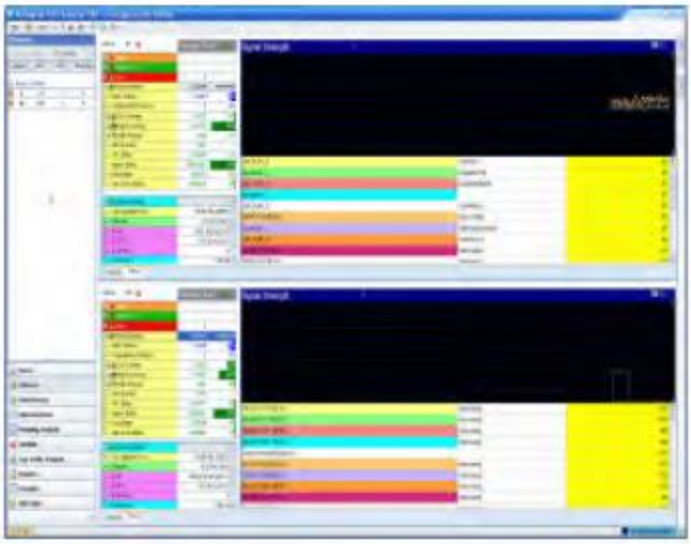
Вид	Страница
Consolidated (Объединенный) Захваченные данные со всех адаптеров анализируются и представляются в одном «виртуальном» виде.	Start (Начать) Roaming Analysis (Анализ роуминга)
Split (Разделенный) Данные и анализ для каждого адаптера представлены на странице в отдельном окне.	Channel (Канал) Decodes (Декодирование)
Adapter Specific (Конкретный адаптер) Данные и анализ для адаптера отображаются индивидуально. Пользователь выбирает, какой адаптер использовать для отображения.	Infrastructure (Инфраструктура) AirWISE Top Traffic Analysis (Анализ трафика по максимальным показателям) Reports (Отчеты) Wi-Fi Tools (Инструменты Wi-Fi)
Not Avaliable (Недоступно)	Interference (Помехи)

Страница Start (Начать)

Страница Roaming Analysis (Анализ роуминга)

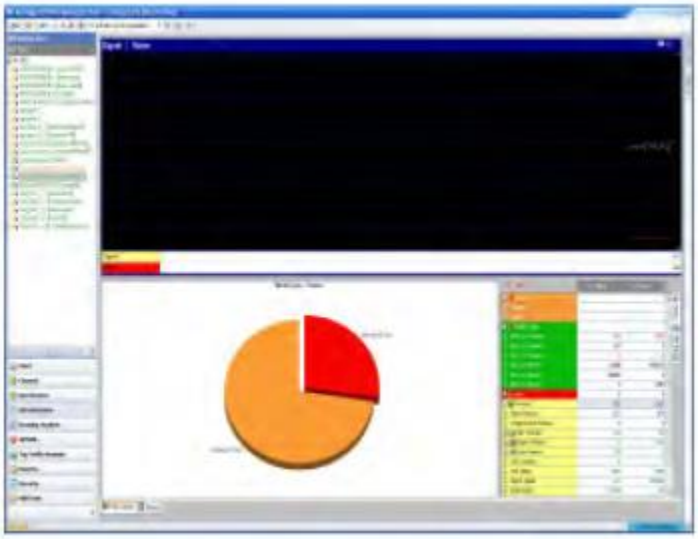


Страница Channel (Канал)



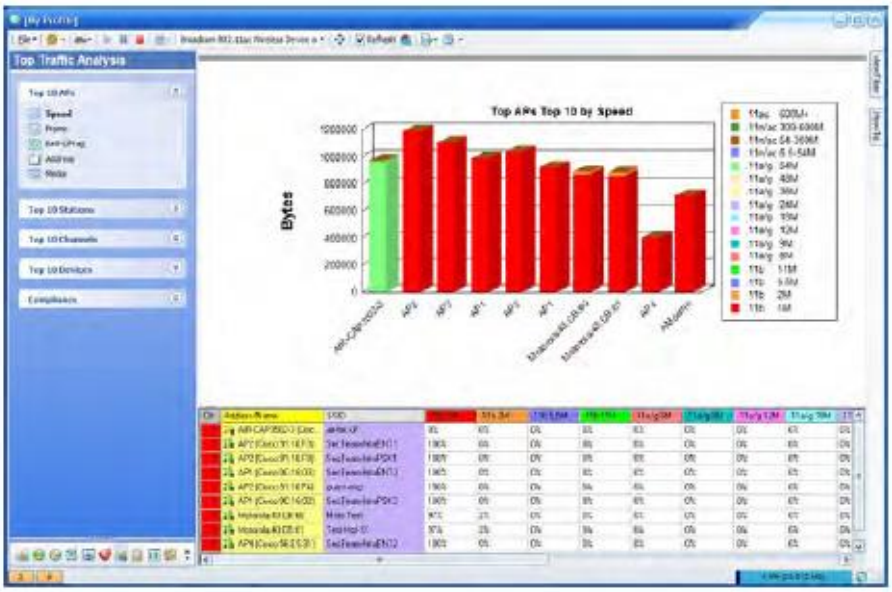
Страница Decades (Декодирование)

Страница Infrastructure (Инфраструктура)



Страница AirWISE

Страница Top Traffic Analysis (Анализ трафика по максимальным показателям)

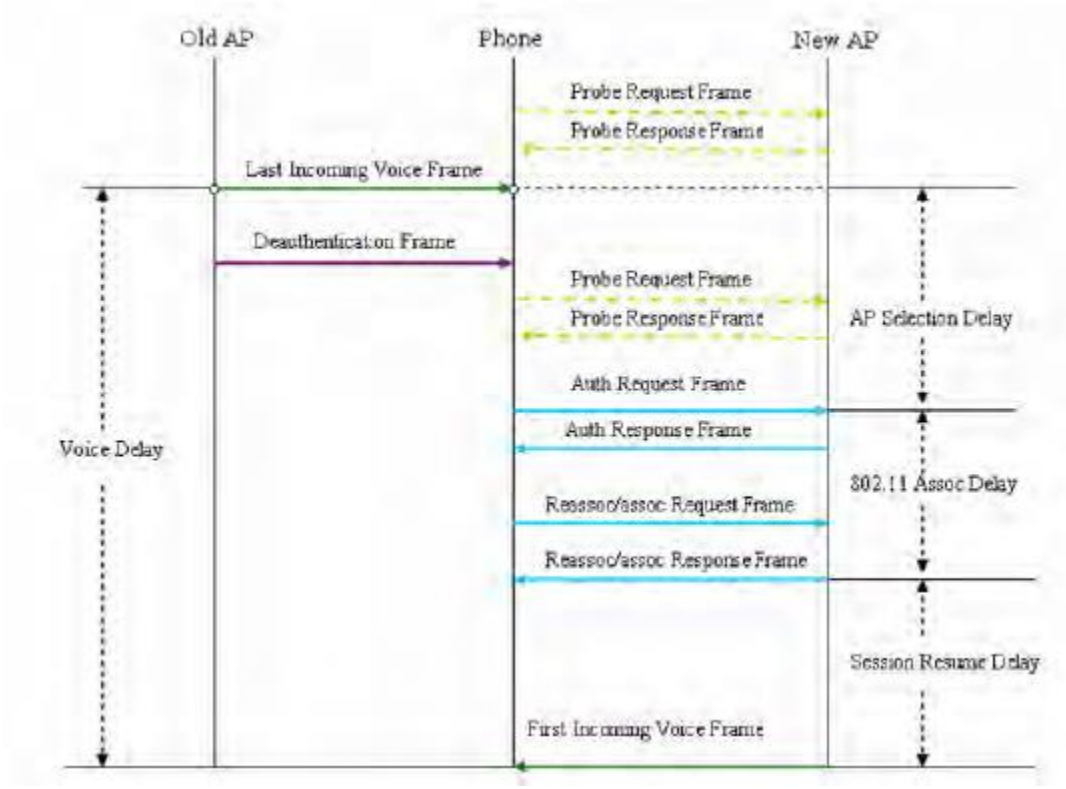


Страница Reports (Отчеты)

Страница Wi-Fi Tools (Инструменты Wi-Fi)

Определение и расчет паузы при роуминге для телефонов Cisco и Vocera

A. Без аутентификации 802.1X

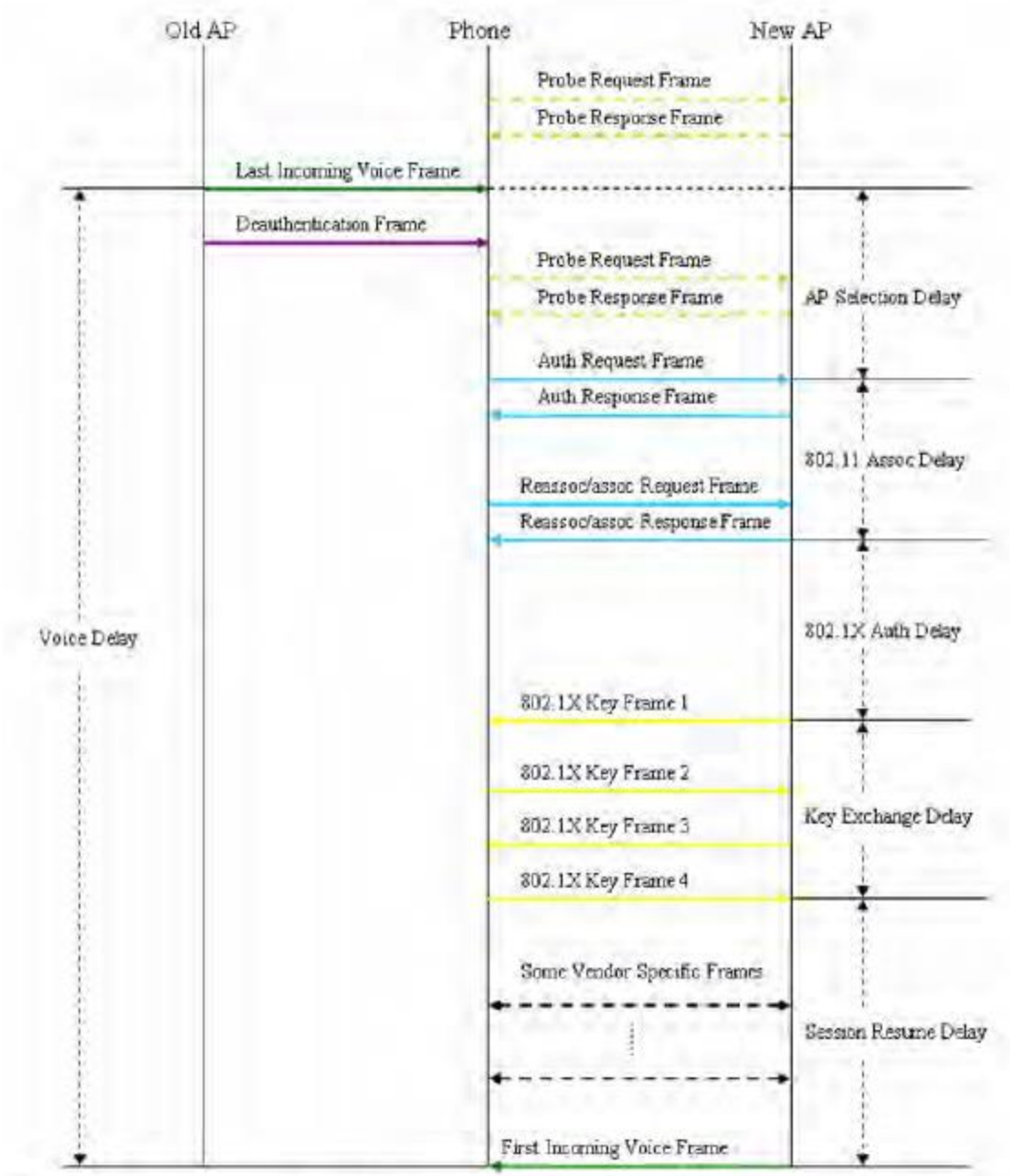


Old AP	Старая точка доступа
Phone	Телефон
New AP	Новая точка доступа
Last Incoming Voice Frame	Последний входящий кадр голосовых данных
Probe Request Frame	Кадр зондирующего запроса
Probe Response Frame	Кадр ответа на зондирующий запрос
Voice Delay	Задержка голоса
Deauthentication Frame	Кадр деаутентификации
AP Selection Delay	Задержка выбора точки доступа
Auth Request Frame	Кадр запроса аутентификации
Auth Response Frame	Кадр ответа на запрос аутентификации
Reassoc/assoc Request Frame	Кадр запроса повторного подключения/подключения
Reassoc/assoc Response Frame	Кадр ответа на запрос повторного подключения/подключения
802.11 Assoc Delay	Задержка подключения 802.11
First Incoming Voice Frame	Первый входящий кадр голосовых данных
Session Resume Delay	Задержка восстановления сеанса

Тип задержки	С кадра	До кадра
Задержка выбора точки доступа	Последний входящий кадр голосовых данных через старую точку доступа / или кадр деаутентификации(если есть)	Первый запрос аутентификации
Задержка подключения 802.11	Первый запрос аутентификации	Последний ответ повторного подключения/подключения
Задержка восстановления сеанса	Последний ответ повторного подключения/подключения	Первый входящий кадр голосовых данных через новую точку доступа
Задержка голоса	Последний входящий кадр голосовых данных через старую точку доступа	Первый входящий кадр голосовых данных через новую точку доступа

Примечания:
Если в качестве начала задержки выбора точки доступа используется последний входящий голосовой вызов со старой точки доступа: Задержка голоса = Задержка выбора точки доступа + Задержка подключения 802.11 + Задержка возобновления сеанса.
Если в качестве начала задержки выбора точки доступа используется кадр деаутентификации: Задержка голоса > Задержка выбора точки доступа + Задержка подключения 802.11 + Задержка возобновления сеанса

Б. С аутентификацией 802.1X



Old AP	Старая точка доступа
Phone	Телефон
New AP	Новая точка доступа
Last Incoming Voice Frame	Последний входящий кадр голосовых данных
Probe Request Frame	Кадр зондирующего запроса
Probe Response Frame	Кадр ответа на зондирующий запрос
Voice Delay	Задержка голоса
Deauthentication Frame	Кадр деаутентификации
AP Selection Delay	Задержка выбора точки доступа
Auth Request Frame	Кадр запроса аутентификации
Auth Response Frame	Кадр ответа на запрос аутентификации
Reassoc/assoc Request Frame	Кадр запроса повторного подключения/подключения
Reassoc/assoc Response Frame	Кадр ответа на запрос повторного подключения/подключения
802.11 Assoc Delay	Задержка подключения 802.11
802.1X Auth Delay	Задержка аутентификации 802.1X
802.1X Key Frame 1 (2, 3, 4)	Кадр 1 (2, 3, 4) ключа 802.1X

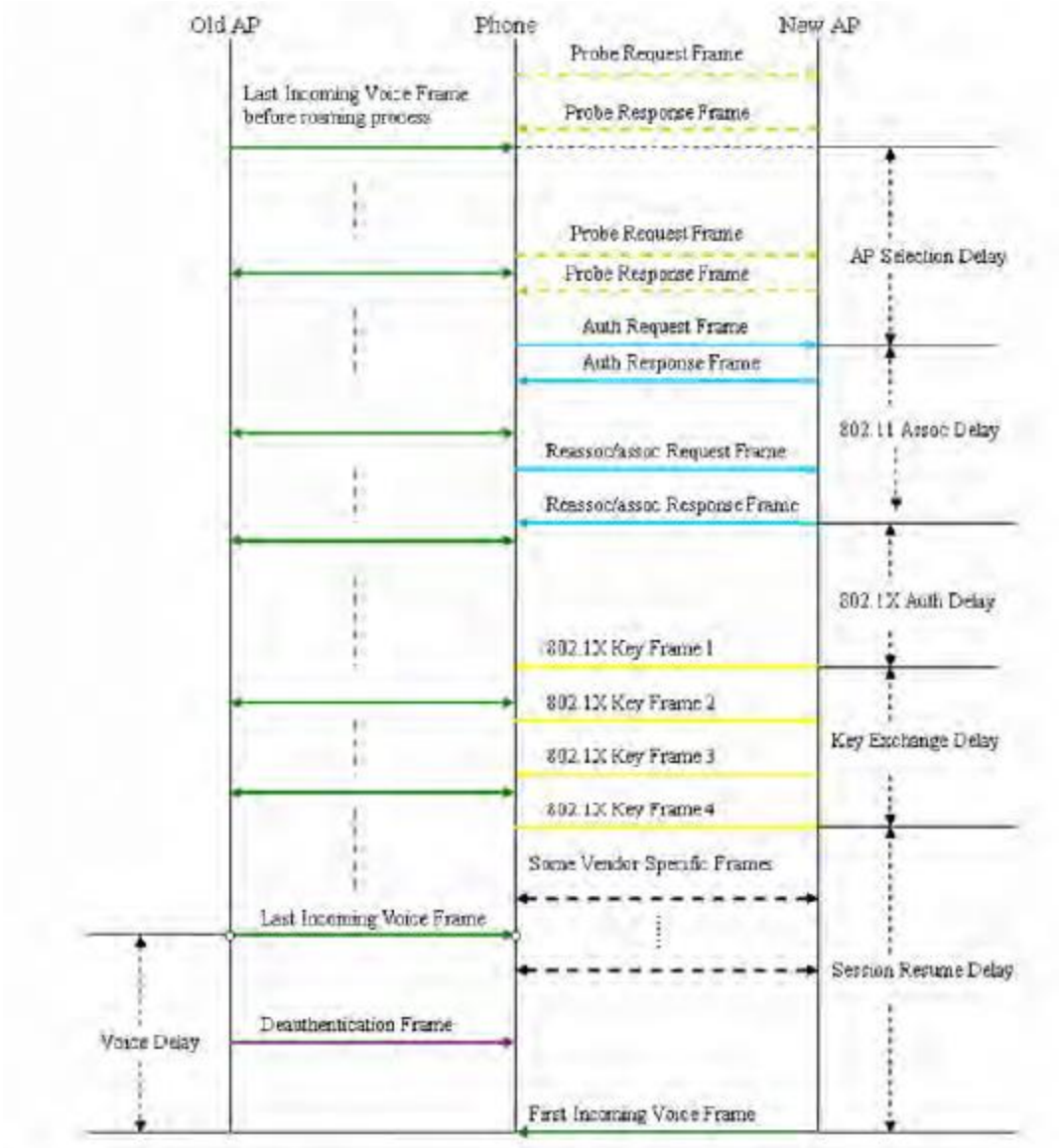
Key Exchange Delay	Задержка обмена ключами
Some Vendor Specific Frame	Специализированный кадр некоторых производителей
First Incoming Voice Frame	Первый входящий кадр голосовых данных
Session Resume Delay	Задержка восстановления сеанса

Тип задержки	С кадра	До кадра
Задержка выбора точки доступа	Последний входящий кадр голосовых данных через старую точку доступа / или кадр деаутентификации(если есть)	Первый запрос аутентификации
Задержка подключения 802.11	Первый запрос аутентификации	Последний ответ повторного подключения/подключения
Задержка аутентификации 802.1X	Последний ответ повторного подключения/подключения	Первый обмен ключами
Задержка обмена ключами	Первый обмен ключами	Последний обмен ключами
Задержка восстановления сеанса	Последний обмен ключами	Первый входящий кадр голосовых данных через новую точку доступа
Задержка голоса	Последний входящий кадр голосовых данных через старую точку доступа	Первый входящий кадр голосовых данных через новую точку доступа

Примечания:
Если в качестве начала задержки выбора точки доступа используется последний входящий голосовой вызов со старой точки доступа: Задержка голоса = Задержка выбора точки доступа + Задержка подключения 802.11 + Задержка возобновления сеанса.
Если в качестве начала задержки выбора точки доступа используется кадр деаутентификации: Задержка голоса > Задержка выбора точки доступа + Задержка подключения 802.11 + Задержка возобновления сеанса

Определение и расчет паузы при роуминге для телефонов SpectraLink

A. С голосовыми кадрами в процессе роуминга



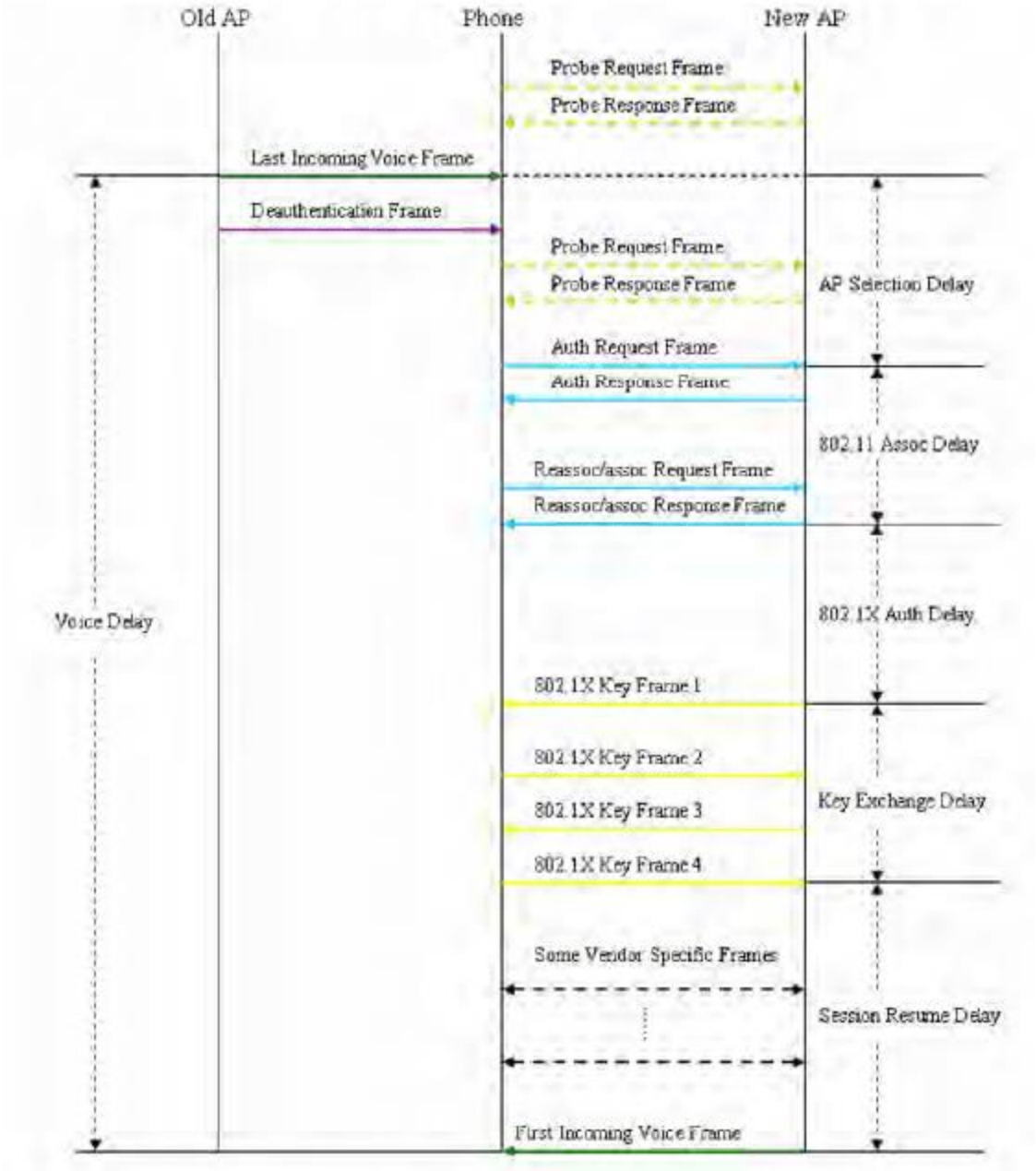
Old AP	Старая точка доступа
Phone	Телефон
New AP	Новая точка доступа
Last Incoming Voice Frame before roaming process	Последний входящий кадр голосовых данных перед процессом роуминга
Probe Request Frame	Кадр зондирующего запроса
Probe Response Frame	Кадр ответа на зондирующий запрос
AP Selection Delay	Задержка выбора точки доступа
Auth Request Frame	Кадр запроса аутентификации
Auth Response Frame	Кадр ответа на запрос аутентификации
802.11 Assoc Delay	Задержка подключения 802.11
Reassoc/assoc Request Frame	Кадр запроса повторного подключения/подключения
Reassoc/assoc Response Frame	Кадр ответа на запрос повторного подключения/подключения
802.1X Auth Delay	Задержка аутентификации 802.1X
802.1X Key Frame 1 (2, 3, 4)	Кадр 1 (2, 3, 4) ключа 802.1X
Key Exchange Delay	Задержка обмена ключами
Last Incoming Voice Frame	Последний входящий кадр голосовых данных
Some Vendor Specific Frame	Специализированный кадр некоторых производителей

Voice Delay	Задержка голоса
Deauthentication Frame	Кадр деаутентификации
Session Resume Delay	Задержка восстановления сеанса
First Incoming Voice Frame	Первый входящий кадр голосовых данных

Тип задержки	С кадра	До кадра
Задержка выбора точки доступа	Последний кадр голосовых данных через старую точку доступа / или кадр деаутентификации(если есть)	Первый запрос аутентификации
Задержка подключения 802.11	Первый запрос аутентификации	Последний ответ повторного подключения/подключения
Задержка аутентификации 802.1X	Последний ответ повторного подключения/подключения	Первый обмен ключами
Задержка обмена ключами	Первый обмен ключами	Последний обмен ключами
Задержка восстановления сеанса	Последний обмен ключами	Первый кадр голосовых данных через новую точку доступа
Задержка голоса	Последний входящий кадр голосовых данных через старую точку доступа	Первый входящий кадр голосовых данных через новую точку доступа
Задержка роуминга	Первый зондирующий запрос	Первый кадр голосовых данных через новую точку доступа

Примечание: В этом случае задержка голоса не является суммой других задержек. Она может быть очень маленькой, поскольку голосовые кадры продолжают проходить в процессе роуминга.

Б. Без голосового кадра в процессе роуминга



Old AP	Старая точка доступа
Phone	Телефон
New AP	Новая точка доступа
Probe Request Frame	Кадр зондирующего запроса
Probe Response Frame	Кадр ответа на зондирующий запрос
Last Incoming Voice Frame	Последний входящий кадр голосовых данных
Deauthentication Frame	Кадр деаутентификации
AP Selection Delay	Задержка выбора точки доступа
Auth Request Frame	Кадр запроса аутентификации
Auth Response Frame	Кадр ответа на запрос аутентификации
802.11 Assoc Delay	Задержка подключения 802.11
Reassoc/assoc Request Frame	Кадр запроса повторного подключения/подключения
Reassoc/assoc Response Frame	Кадр ответа на запрос повторного подключения/подключения
Voice Delay	Задержка голоса
802.1X Auth Delay	Задержка аутентификации 802.1X
802.1X Key Frame 1 (2, 3, 4)	Кадр 1 (2, 3, 4) ключа 802.1X
Key Exchange Delay	Задержка обмена ключами

Some Vendor Specific Frame	Специализированный кадр некоторых производителей
Session Resume Delay	Задержка восстановления сеанса
First Incoming Voice Frame	Первый входящий кадр голосовых данных

Тип задержки	С кадра	До кадра
Задержка выбора точки доступа	Последний входящий кадр голосовых данных через старую точку доступа / или кадр деаутентификации(если есть)	Первый запрос аутентификации
Задержка подключения 802.11	Первый запрос аутентификации	Последний ответ повторного подключения/подключения
Задержка аутентификации 802.1X	Последний ответ повторного подключения/подключения	Первый обмен ключами
Задержка обмена ключами	Первый обмен ключами	Последний обмен ключами
Задержка восстановления сеанса	Последний обмен ключами	Первый входящий кадр голосовых данных через новую точку доступа
Задержка голоса	Последний входящий кадр голосовых данных через старую точку доступа	Первый входящий кадр голосовых данных через новую точку доступа

Примечания:
Если в качестве начала задержки выбора точки доступа используется последний входящий голосовой вызов со старой точки доступа: Задержка голоса = Задержка выбора точки доступа + Задержка подключения 802.11 + Задержка возобновления сеанса.
Если в качестве начала задержки выбора точки доступа используется кадр деаутентификации: Задержка голоса > Задержка выбора точки доступа + Задержка подключения 802.11 + Задержка возобновления сеанса

Конфигурация системы

Настройка приложения AirMagnet WiFi Analyzer

Для эффективного решения проблем с сетью с помощью приложения AirMagnet WiFi Analyzer сначала необходимо убедиться в правильности настройки различных системных параметров приложения. Все настройки системы выполняются в диалоговом окне Configuration (Конфигурация), в верхней части которого имеется ряд вкладок, каждая из которых представляет собой определенный системный параметр.

Все настройки конфигурации системы приложения AirMagnet WiFi Analyzer сохраняются в профиле по умолчанию под названием My Profile (Мой профиль). Это облегчает вызов настроек конфигурации для обследования каждой площадки. Настройки конфигурации можно сохранить для любого места или площадки для администрирования беспроводной локальной сети. Также параметры конфигурации можно экспортировать в виде шаблонов, которые впоследствии можно будет импортировать для использования в других обследованиях.

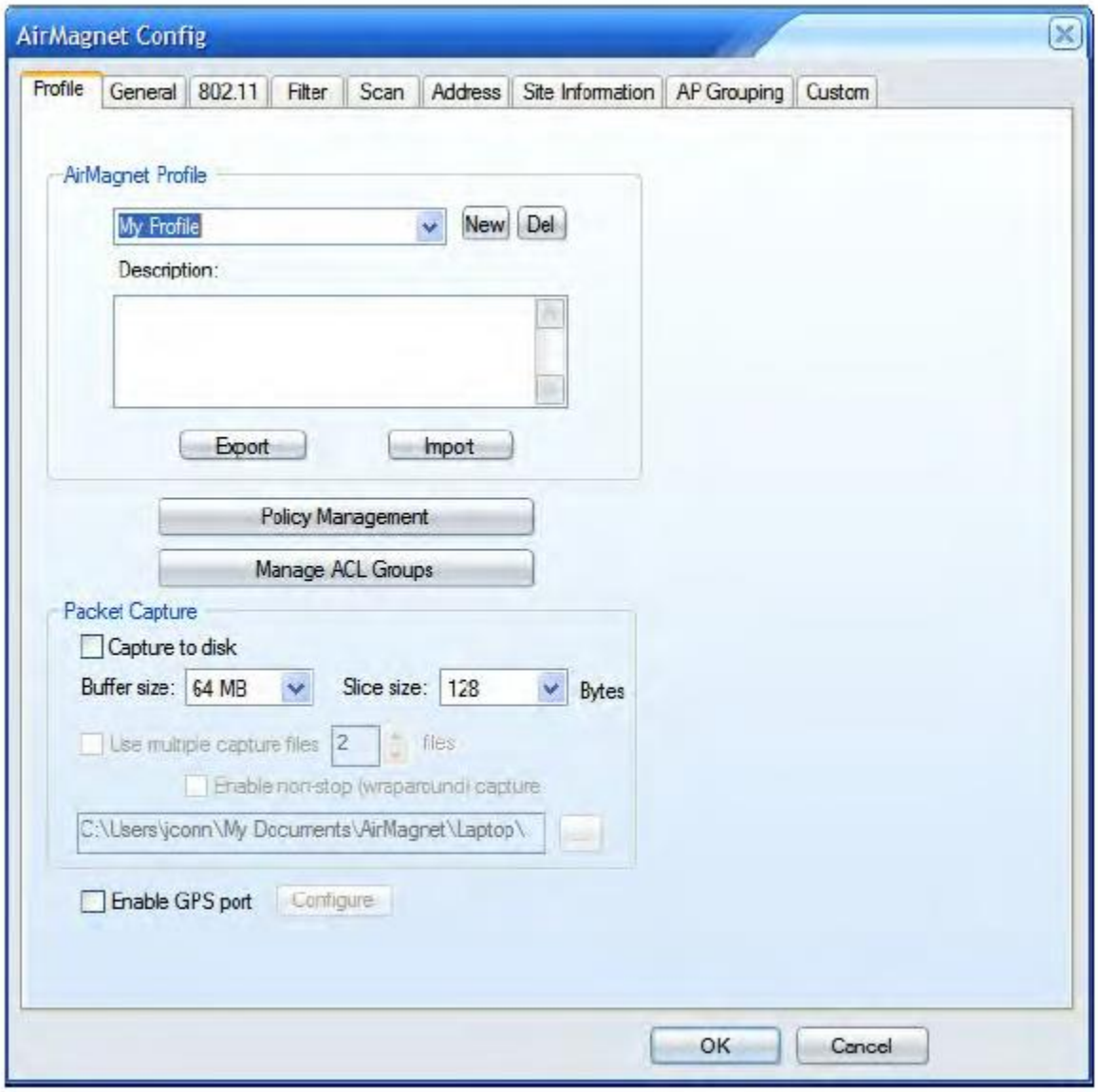
Если ваша ответственность как администратора беспроводной локальной сети охватывает более одного объекта или если вы обслуживаете более одного клиента, то для вас утилита AirMagnet Configuration Profile станет очень полезной в деле управления различными параметрами конфигурации.

Интеграция с профилями беспроводной связи Windows описывается в разделе «Интеграция с беспроводной конфигурацией Windows».

Для получения доступа к экрану AirMagnet Configuration (Конфигурация AirMagnet) выполните одно из следующих действий на панели меню:

- Дважды щелкните кнопкой мыши на  (Настроить).
- Выберите File > Configure (Файл > Настроить).

Откроется диалоговое окно AirMagnet Configuration (Конфигурация AirMagnet). Диалоговое окно AirMagnet Configuration по умолчанию показано на рисунке ниже.



Примечание: По умолчанию при открытии диалогового окна AirMagnet Configuration (Конфигурация AirMagnet) выделяется вкладка Profile (Профиль). Чтобы посмотреть или настроить любой системный параметр, откройте соответствующую вкладку в верхней части диалогового окна.

Настройка системного профиля

В этом разделе объясняется, как создать системный профиль приложения AirMagnet WiFi Analyzer. После создания такой профиль будет использоваться в качестве шаблона, в соответствии с которым упорядочиваются все системные параметры, что упрощает архивирование, извлечение или совместное использование этих данных.

Примечание: После настройки имя профиля будет отображаться на панели заголовка экранов. Если никакой профиль не был настроен, вместо его имени на панели заголовка отображается имя профиля по умолчанию [My Profile (Мой профиль)].

Import (Импортировать): Если доступен ранее созданный профиль, его можно импортировать. Нажмите Import (Импортировать) и найдите файл .APF.
Export (Экспортировать): Текущий системный профиль можно экспортировать. Нажмите Export (Экспортировать). Введите имя файла и откройте желаемое место его сохранения. Нажмите Save (Сохранить).

Для настройки системного профиля приложения AirMagnet WiFi Analyzer:

1. Убедитесь, что в диалоговом окне AirMagnet Configuration (Конфигурация AirMagnet) выбрана вкладка Profile (Профиль).
2. Выберите New (Создать) и замените надпись [Mew Profile] (Новый профиль) уникальным именем профиля.
3. Щелкните кнопкой мыши на поле Description (Описание) и введите описание этого профиля.
4. Щелкните кнопкой мыши на Policy Management (Управление политиками), чтобы установить политику профиля. Дополнительная информация приводится в разделе «Управление сетевыми политиками».
5. Чтобы настроить группы ACL (Список контроля доступа) профиля, щелкните кнопкой мыши на Manage ACL Groups (Управлять группами ACL). Для получения дополнительной информации обратитесь к разделу «Назначение политик группам ACL».

Захват пакетов (Packet Capture):

6. Для захвата пакетных данных на диск можно использовать любой из трех выбираемых способов: захват на диск, использование нескольких файлов захвата и включение непрерывного захвата.
   Capture to Disk (Захват на диск): Поставьте метку в этом поле, чтобы захватывать и сохранять пакетные данные с максимальным размером файла, выбранным в разворачивающемся списке File size (Размер файла). Также можно выбрать размер вырезки в байтах в разворачивающемся списке Slice size (Размер вырезки). Захват останавливается по достижении размера буферной памяти.
   При достижении указанного размера буферной памяти появляется диалоговое окно, в котором предоставляется возможность выбора места сохранения файла на диск.

   Use multiple capture files (Использовать несколько файлов захвата): Поставив метку также и в этом поле, можно установить количество нескольких последовательных файлов захвата, размер каждого из которых был указан для Capture to disk (Захват на диск). Каждый файл получит имя с отметкой времени окончания захвата (например, July 12, 2011-1410.amm). Файл будет сохранен в папку, указанную в поле Browse. Место сохранения по умолчанию airmagnet/laptop.

   Enable non-stop (wrap-around) capture (Включить непрерывный (циклический) захват): Установка метки в этом поле включает режим непрерывного захвата. Это означает, что при достижении установленного количества «нескольких файлов захвата» самый старый файл будет автоматически удален, чтобы сохранить новый файл. При использовании этого метода пакетные данные захватываются непрерывно, а общее количество файлов ограничено числом, установленным для Use multiple capture files (Использовать несколько файлов захвата). Непрерывный захват продолжается, пока не будет снята метка из этого поля.

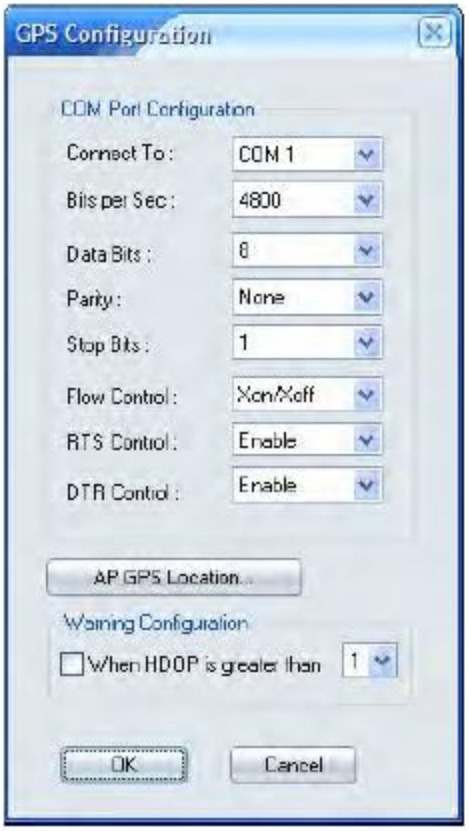
Также можно установить метку в поле Enable GPS port (Включить порт GPS), чтобы использовать соответствующую функцию, а затем нажать Configure (Настроить) для выполнения настройки GPS.

7. Для завершения настройки профиля нажмите кнопку OK.

Примечание: Если профиль уже существует, для его поиска и импортирования нажмите Import (Импортировать). При желании можно экспортировать профиль для ведения учета или совместного использования с другими пользователями.

Настройка параметров GPS

Если в поле Enable GPS port (Включить порт GPS) установлена метка, а затем нажата кнопка Configure (Настроить), появится показанное на рисунке ниже диалоговое окно GPS Configuration (Настройка конфигурации GPS). Диалоговое окно представляет собой интерфейс настройки порта, который приложение AirMagnet WiFi Analyzer будет использовать для связи с устройством GPS.

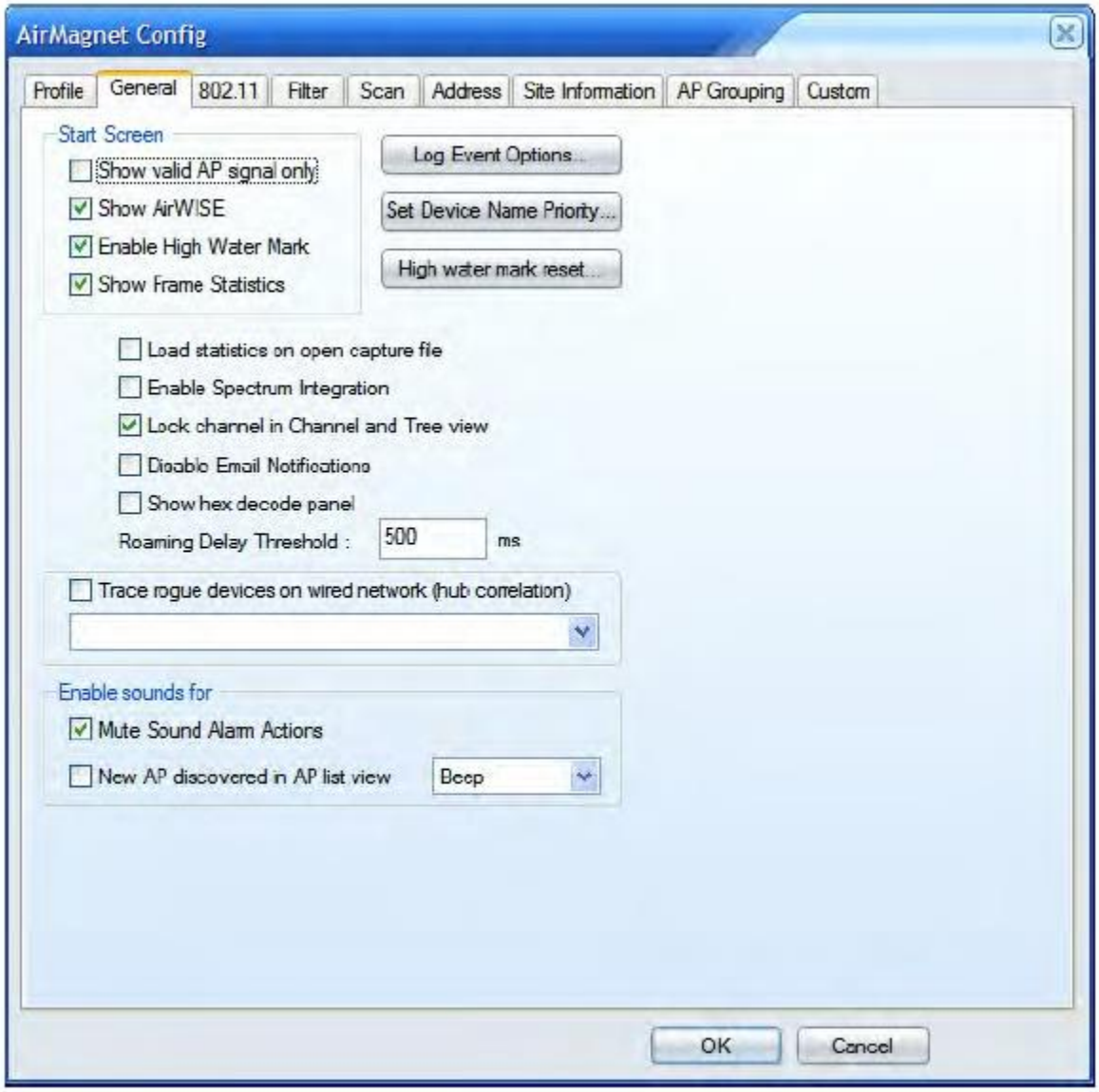


Для настройки порта GPS:

1. Сделайте желаемый выбор в диалоговом окне.
2. Нажмите кнопку AP GPS Location (Местоположение точки доступа по GPS), чтобы настроить местоположение GPS нужных точек доступа в сети, как показано в разделе «Получение информации о местоположении точек доступа по GPS».

Настройка общих системных параметров

На вкладке General (Общие) представлены параметры, определяющие общее функционирование приложения AirMagnet WiFi Analyzer. При первом открытии приложения после установки отображаются настройки по умолчанию. Любой из параметров можно изменить в любое время в соответствии с потребностями вашей беспроводной локальной сети.



Для настройки общих параметров приложения AirMagnet WiFi Analyzer:

1. В диалоговом окне AirMagnet Configuration выберите вкладку General (Общие).
2. Сделайте требуемый выбор, как описано в таблице ниже.
3. По завершении нажмите кнопку OK.

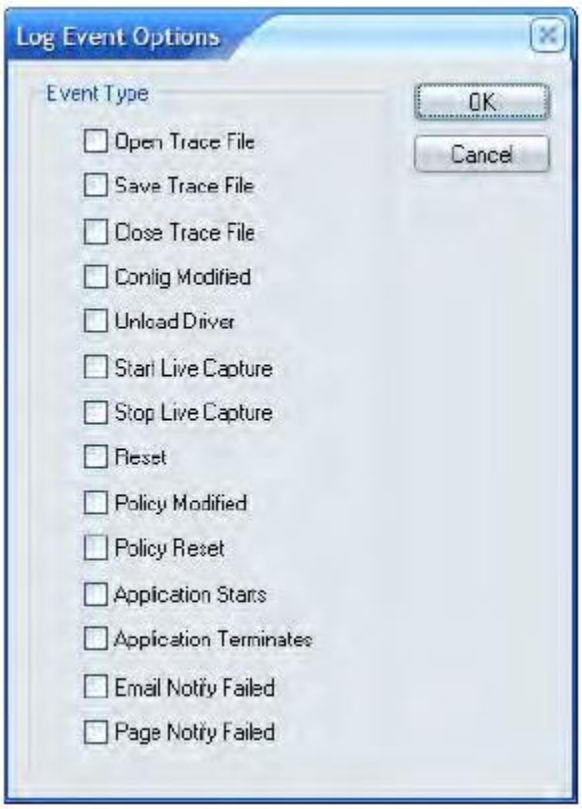
Параметр	Описание
Show valid AP signal only (Показывать только сигнал легитимной точки доступа)	Если поставлена метка в этом поле, система не будет отображать на графике сигнала на экране Start коричневые полосы, представляющие межканальные помехи.
Show AirWISE (Показывать AirWISE)	Если поставлена метка в этом поле, внизу в средней части экрана Start появится панель AirWISE.
Enable High Water Mark (Включить высшую точку)	Если поставлена метка в этом поле, на графиках в верхнем левом углу экрана Start в течение заданного пользователем интервала времени будет сохраняться высшая точка. Это позволяет видеть высшую точку, достигнутую сетевым трафиком

	за заданное время. Чтобы указать это время, нажмите кнопку сброса высшей точки экрана Start (High water mark reset).
Show Frame Statistics (Показывать статистику кадров)	Если выбран этот параметр, под круговой диаграммой на экране Start появится панель подсчета кадров.
	Примечание: Для отображения статистики кадров требуется экран большего размера.
Load statistics on open capture files (Загрузить статистику открытых файлов захвата)	Если поставлена метка в этом поле, для загруженного файла захвата будет отображаться вся информация, которая была захвачена во время сохраненного сеанса. При обычном воспроизведении будут отображаться только обнаруженные устройства до тех пор, пока не будет заполнен буфер захвата; эта опция позволяет просматривать устройства, которые были зарегистрированы ранее, но затем перезаписаны по мере заполнения буфера.
Enable Spectrum Integration (Включить интеграцию с Spectrum)	Если поставлена метка в этом поле, будет включена интеграция с AirMagnet Spectrum XT. Более подробная информация приводится в разделе «Интеграция с анализатором спектра AirMagnet».
Lock Channel in Channel and Tree view (Зафиксировать канал на экране канала и дерева)	Если поставлена метка в этом поле, система прекратит сканирование других каналов при детальном просмотре выбранного канала на экране Channel (Канал).
Disable Email Notification (Отключить уведомление по электронной почте)	Если выбран этот параметр, система не будет отправлять уведомления по электронной почте.
Show hex decode panel (Показать панель шестнадцатеричного декодирования)	Если поставлена метка в этом поле, на экране Decodes (Декодирование) будет отображаться шестнадцатеричная панель.
Roaming Delay Threshold (Порог задержки роуминга)	Разница между временем начала и окончания переключения в роуминге. Как правило, только для голосового роуминга, если задержка превышает пороговое значение задержки голосового роуминга, отображается значок с направленным вниз большим пальцем.
Trace rogue devices on wired network (Отслеживать неавторизованные устройства на проводной сети)	Если поставлена метка в этом поле, система будет отслеживать неавторизованные устройства на проводной стороне сети. Во время активного отслеживания приложение AirMagnet WiFi Analyzer попытается отследить все неавторизованные устройства, подключенные к тому же концентратору, что и компьютер Wi-Fi.
	Примечание: Для использования этой опции ваш ноутбук должен быть подключен через Ethernet.
Mute sound alarm actions (Отключить звуковой сигнал тревоги)	Если поставлена метка в этом поле, система не будет подавать звуковой сигнал при создании нового сигнала тревоги.
New AP discovered in AP list view (На панели списка точек доступа обнаружена новая точка доступа)	Если поставлена метка в этом поле, система будет подавать звуковой сигнал при обнаружении новой точки доступа.
	Примечание: Чтобы выбрать настройку звука в меню списка, щелкните кнопкой мыши на направленной вниз стрелке.

Настройка параметров журнала событий (Log Event Options)

Данная опция позволяет указать действия приложения AirMagnet WiFi Analyzer, которые будут записываться в журнал событий Windows. Хотя включение всех этих опций позволит вести учет всех исторических данных или событий, записанных приложением AirMagnet WiFi Analyzer, также это может привести к быстрому потреблению большого объема дискового пространства.

1. Щелкните кнопкой мыши на Log Events Options (Опции журнала событий).
2. Выберите опции, которые хотите записывать.
3. Нажмите кнопку ОК.



Настройка приоритета отображения имени устройства (Set Device Name Priority)

Данная опция позволяет установить порядок приоритета отображения устройств на экране.

1. Щелкните кнопкой мыши на Set device name priority (Установить приоритет имени устройства).
2. Выделяйте опции по очереди и устанавливайте их приоритет с помощью стрелки, направленной вверх и/или вниз.
3. По завершении нажмите кнопку OK.

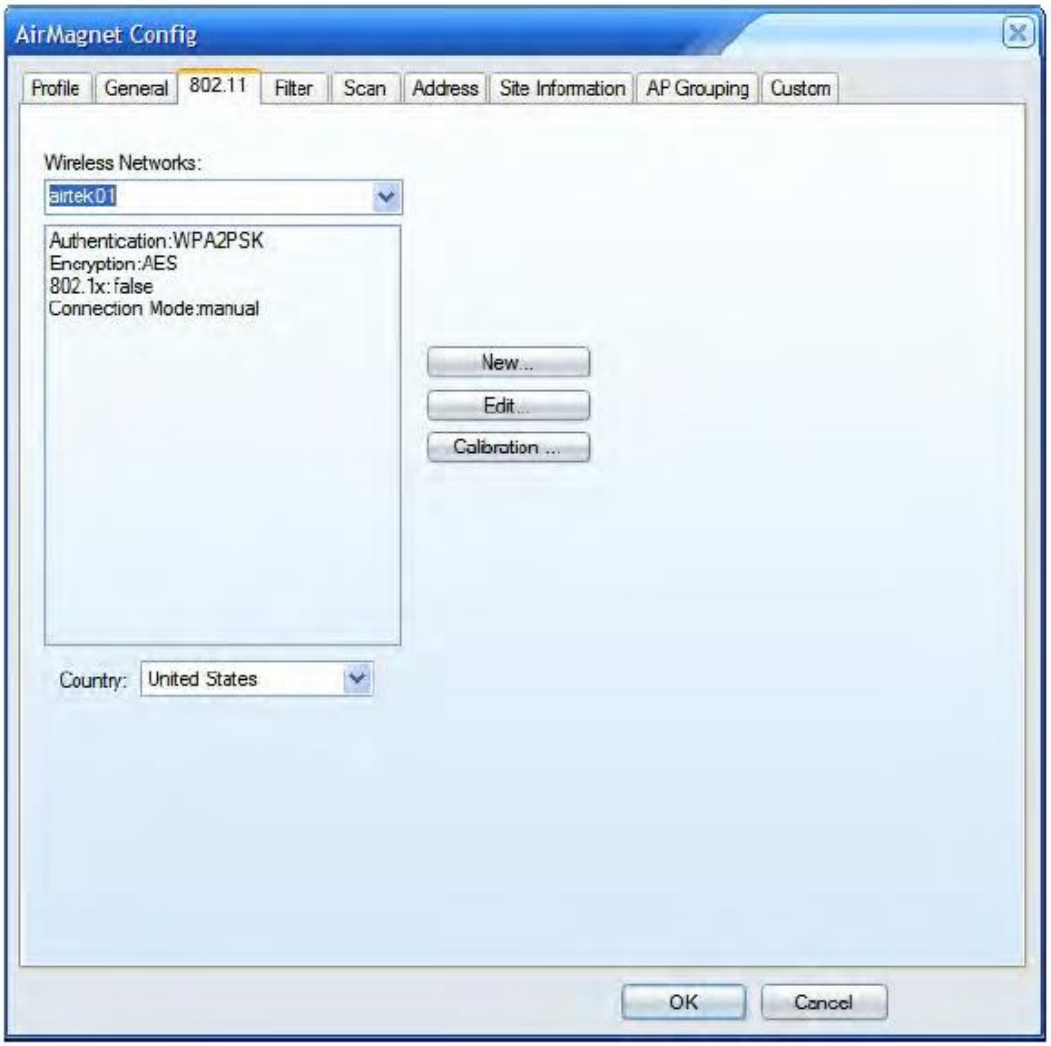
Сброс высшей точки (High Water Mark Reset)

Нажмите эту кнопку, чтобы сбросить высшую точку.

1. Щелкните кнопкой мыши на High water mark reset (Сброс высшей точки).
2. Выберите опцию сброса.
3. Нажмите кнопку OK.

Настройка параметров 802.11

Экран конфигурации 802.11 позволяет установить параметры для включения активного соединения с точкой доступа на сети. Перед использованием любого из таких активных инструментов, как One Touch Connection Test (Тестирование подключения одним нажатием) или Site Survey Tool (Инструмент обследования площадки), необходимо настроить хотя бы одну беспроводную сеть.



Данная процедура позволяет установить пароль аутентификации и безопасности для точки доступа или SSID. Перечень доступных опций зависит от используемого адаптера и операционной системы.

Примечание: Это также можно сделать в Windows, настроив беспроводное сетевое соединение.

1. Откройте окно Configure (Настроить) и щелкните кнопкой мыши на вкладке 802.11.
2. Для создания нового профиля нажмите New (Создать). Введите правильное имя для точки доступа или SSID и нажмите OK.
3. Выбрав SSID или имя точки доступа в разворачивающемся списке Wireless Networks (Беспроводные сети), нажмите Edit (Изменить).
4. Введите нужные записи и/или сделайте выбор на вкладках Connections (Подключения) и Security (Безопасность) как для обычного нового беспроводного подключения Windows.
5. Нажмите кнопку OK.

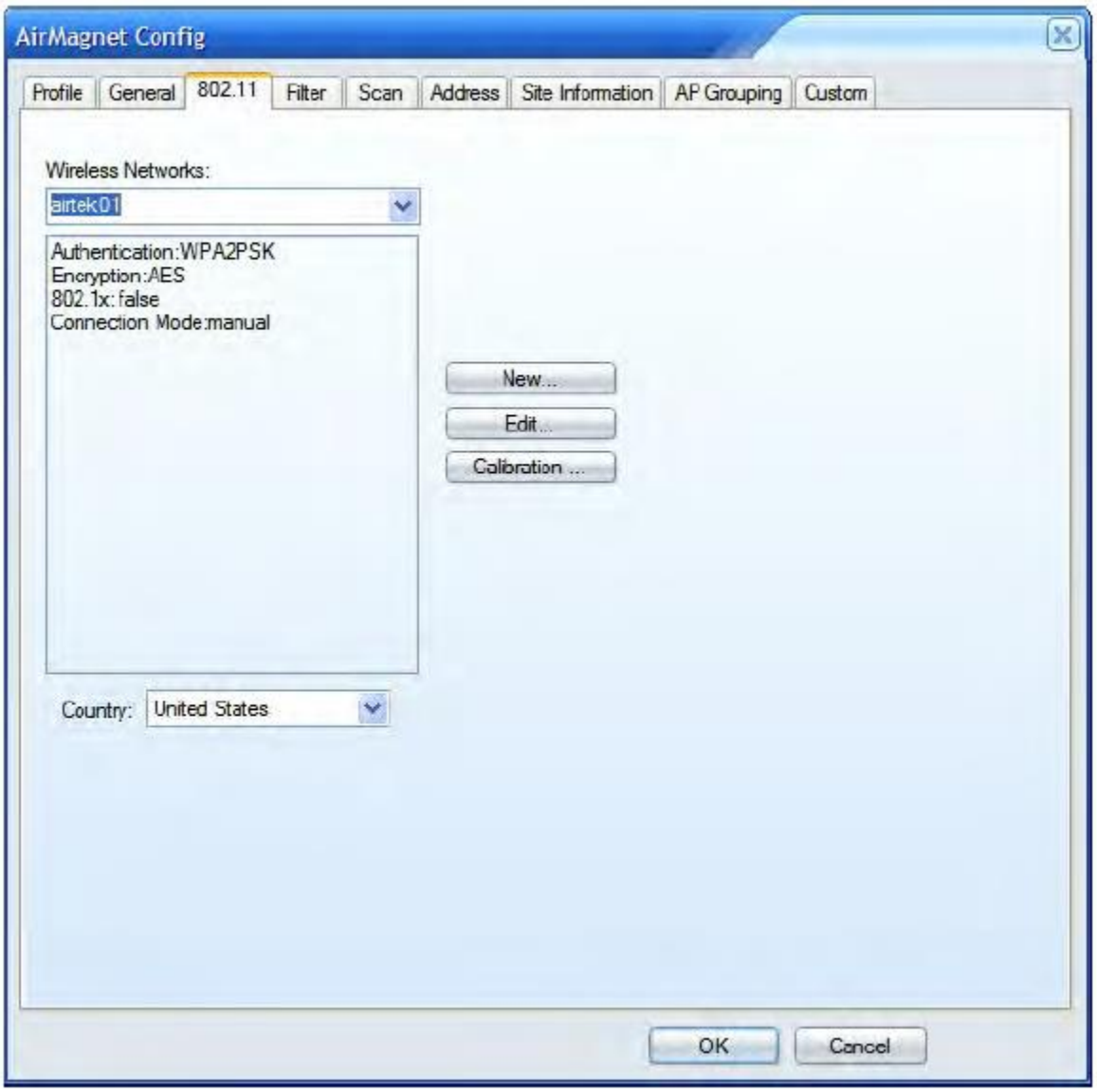
Калибровка радиочастотного сигнала

О радиочастотной калибровке

Для использования с различными приложениями на выбор доступно множество беспроводных сетевых адаптеров стандарта 802.11. Так как эти адаптеры разрабатываются и выпускаются разными производителями, между ними существует вероятность производственных различий, которые могут привести к разности в показаниях сигналов.

Являясь лидером в области анализа и устранения неисправностей сетей Wi-Fi, компания AirMagnet создала программу калибровки и тестирования, охватывающую большую часть нашего «предпочтительного» списка адаптеров Wi-Fi, приведенного на веб-сайте AirMagnet (http://www.airmagnet.com/support/supported_adapters/). Программа охватывает множество производителей карт и включает обширное тестирование всех каналов Wi-Fi, различных операционных систем и различных уровней мощности/затухания. Насколько нам известно, это наиболее обширное тестирование такого рода в отрасли, которое гарантирует точность ваших измерений с помощью приложения AirMagnet, а также обеспечивает гибкость и экономичность использования готовых беспроводных адаптеров. Компания AirMagnet обновила свои продукты с учетом этих результатов для обеспечения высочайшего уровня точности продуктов и предоставления своим клиентам наиболее точных и надежных измерений на рынке.

Как использовать опции радиочастотной калибровки в приложении AirMagnet WiFi Analyzer



Приложение AirMagnet WiFi Analyzer имеет диалоговое окно RF Calibration (Радиочастотная калибровка), позволяющее быстро и просто провести калибровку адаптера беспроводной сети. Чтобы открыть это диалоговое окно (смотрите рисунок ниже), сделайте следующее:

- Нажмите File > Configure… > 802.11 > Calibration… (Файл > Настроить> 802.11> Калибровка) или
- Нажмите Configure > 802.11 > Calibration… (Настроить > 802.11 > Калибровка).

В открытом диалоговом окне RF Calibration щелкните кнопкой мыши на направленной вниз стрелке в верхнем левом углу и выберите один из следующих вариантов:

- No Calibration (Без калибровки)
- Pre-Defined Calibration (Предварительно заданная калибровка) (это запись под No Calibration, например, AirMagnet 802.11 a/b/g/n Wireless PC card)
- Custom Calibration (Пользовательская калибровка)

Импортирование/экспортирование конфигурации калибровки

Измененные конфигурации калибровки можно импортировать и экспортировать (не применимо к No Calibration (Без калибровки)). Данная функция позволяет обмениваться настройками калибровки адаптера между приложениями AirMagnet WiFi Analyzer (версия 10.7.1 или выше).

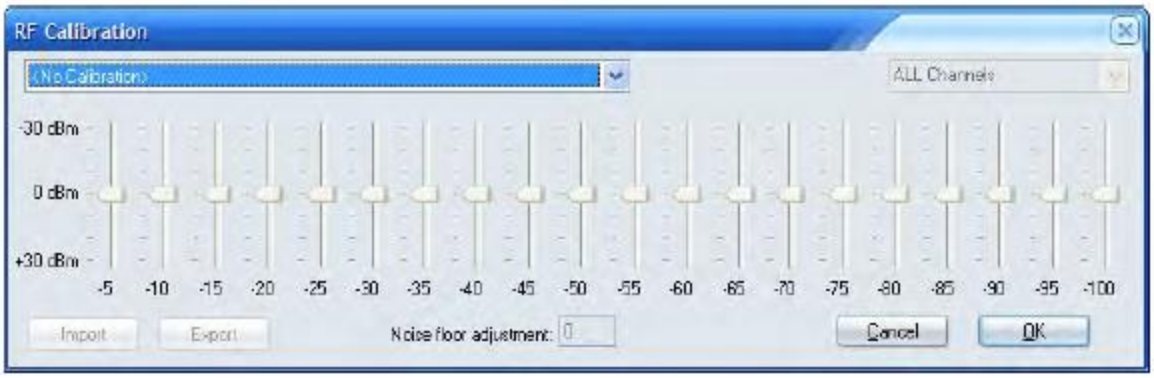
1. В меню File (Файл) нажмите Configure (Настроить).

2. Откройте вкладку 802.11. Щелкните кнопкой мыши на Calibration (Калибровка).
3. В разворачивающемся списке RF Calibration (Радиочастотная калибровка) выберите Pre-Defined Calibration (Предварительно заданная калибровка) или Custom Calibration (Пользовательская калибровка).
4. Для импортирования нажмите Import. Найдите и выберите нужный файл (с расширением .ini). Нажмите Open (Открыть).
5. Для экспортирования нажмите Export. Присвойте файлу имя и перейдите в желаемое место сохранения. Нажмите Save (Сохранить).

No Calibration (Без калибровки)

Выбор опции No Calibration (Без калибровки) означает, что AirMagnet не будет применять к адаптеру беспроводной сети какую-либо коррекцию. Данная опция применяется, когда пользователь предпочитает использовать необработанные показания мощности радиосигнала от производителя адаптера.

Для использования настроек беспроводного сетевого адаптера по умолчанию без калибровки сделайте следующее:
1. В верхнем левом углу диалогового окна RF Calibration (радиочастотная калибровка) щелкните кнопкой мыши на направленной вниз стрелке и выберите в меню No Calibration (Без калибровки). Смотрите рисунок ниже.



Примечание: Если выбрана опция No Calibration (Без калибровки), все остальные элементы управления в диалоговом окне радиочастотной калибровки будут неактивны (недоступны).

2. Для подтверждения выбора нажмите кнопку OK.

Pre-Defined Calibration (Предварительно заданная калибровка)

Если используемый беспроводной сетевой адаптер находится в списке предварительно откалиброванных адаптеров, приложение AirMagnet автоматически распознает его и отобразит вариант предварительно заданной калибровки. Другими словами, если ваш беспроводный сетевой адаптер отображается в меню как Pre-Defined Calibration, значит, существует возможность выбора и использования калиброванных значений AirMagnet. В этом случае вам не нужно ничего делать, кроме выбора этого адаптера. При этом по-прежнему сохраняется возможность внесения изменений в настройки предварительно откалиброванного адаптера беспроводной сети. В этом случае проводится пользовательская настройка предварительно откалиброванного адаптера беспроводной сети, которая будет описана ниже.

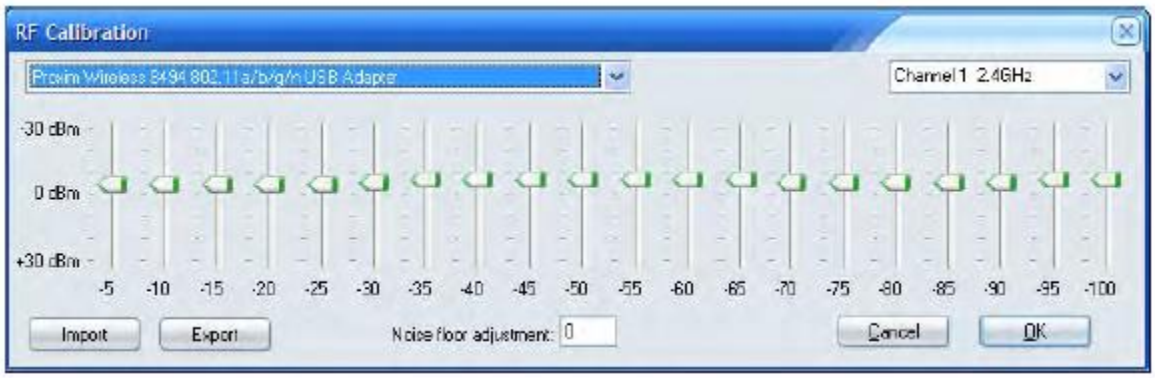
Для обеспечения максимальной точности все тесты для определения откалиброванных значений для беспроводного адаптера проводились с использованием откалиброванных анализаторов спектра в профессионально экранированной изолирующей камере. При калибровке анализатор спектра сначала использовался для измерения мощности радиосигнала нисходящего канала (от точки доступа к станции) от точки доступа в различных точках затухания с аттенюатором, размещенным между ними. Ослабление достигается за счет уменьшения мощности радиосигнала, который аттенюатор получает от точки доступа. Например, если аттенюатор получает от точки доступа сигнал с уровнем -20 дБм, то понижает его до -30 дБм. В результате при приеме анализаторами спектра уровень сигнала точки доступа составит -30 дБм. Измерения выполняются на всех каналах протокола 802.11, используемых на калибруемом адаптере беспроводной сети. После того, как с помощью анализатора спектра установлены эталонные значения, те же процедуры измерения выполняются с беспроводным сетевым адаптером стандарта 802.11 (например,

AirMagnet 802.11 a/b/g/n Wireless PC Card), и значения корректируются в соответствии с эталонными значениями.

Рассмотрим пример. Если в точке затухания А анализатор спектра отображает значение мощности радиосигнала -20 дБм, а калибруемый адаптер показывает -30 дБм, AirMagnet добавляет 10 дБм, чтобы привести его в соответствие с эталонными значениями. Предварительно заданные смещения относятся к анализатору спектра. Другими словами, предварительно заданные шаблоны калибровки заставят целевой адаптер Wi-Fi сообщать значения мощности сигнала, аналогичные показателям профессиональных анализаторов спектра. Для одного и того же адаптера беспроводной сети эта же процедура повторяется для каждого применимого канала/частоты. Таким получаются предварительно заданные значения калибровки. Все данные калибровки для этих предварительно откалиброванных адаптеров беспроводной сети включены в приложение.

Для использования предварительно заданной калибровки сделайте следующее:

1. Щелкните кнопкой мыши на направленной вниз стрелке и убедитесь, что ваш беспроводный сетевой адаптер отображается как запись Pre-Defined Calibration (Предварительно заданная калибровка). Смотрите рисунок ниже.



2. Выберите беспроводный сетевой адаптер, если его имя отображается в списке (например, AirMagnet 802.11 a/b/g/n/ Wireless PC Card, как показано на рисунке выше).
3. Нажмите кнопку OK.

Примечание: Три описанных выше шага – это всё, что нужно сделать пользователю, если адаптер беспроводной сети был идентифицирован приложением AirMagnet как Pre-Defined Calibration (Предварительно заданная калибровка). Никаких других действий не требуется. Однако это не означает, что пользователь не может вносить какие-либо изменения в предварительно откалиброванный адаптер беспроводной сети. Напротив, AirMagnet позволяет пользователю вносить изменения в предварительно откалиброванный адаптер беспроводной сети. В этом случае фактически выполняется пользовательская калибровка на основе предварительно заданной калибровки. Любая пользовательская калибровка, выполненная таким образом, не изменит никаких значений сигналов, которые зависят от настроек предварительной калибровки. Вместо этого она обновляет опцию пользовательской калибровки новыми настройками. В следующем абзаце будет описано, как внести изменения в настройки предварительно откалиброванного адаптера беспроводной сети.

Для внесения изменений в предварительно заданную калибровку сделайте следующее:

1. Повторите шаги с 1 по 2 из предыдущего раздела.
2. Щелкните кнопкой мыши на направленной вниз стрелке в правом верхнем углу и выберите нужный канал.
3. Увеличивайте или уменьшайте мощность радиосигнала с помощью ползунков.
4. Когда появится сообщение Create a custom RF calibration based on current settings? (Создать пользовательскую калибровку радиочастотного сигнала на основе текущих настроек?), нажмите Yes (Да).
5. Продолжайте регулировать уровень сигнала с помощью ползунков.
6. Установите уровень собственных шумов, введя желаемое значение в соответствующем поле.
7. Для применения изменений нажмите кнопку OK.

Примечание: Пользовательская калибровка радиочастотного сигнала на предварительно откалиброванном адаптере беспроводной сети должна выполняться поканально, каждый раз только для одного канала. Это связано с тем, что внесенные в конкретный канал изменения применяются

только к этому каналу. Если необходимо внести изменения в какие-либо другие каналы, используйте ту же процедуру для другого канала.

Custom Calibration (Пользовательская калибровка)

Пользовательскую калибровку можно использовать, если необходимо создать свою собственную таблицу калибровки для адаптера беспроводной сети из диалогового окна RF Calibration (Радиочастотная калибровка).

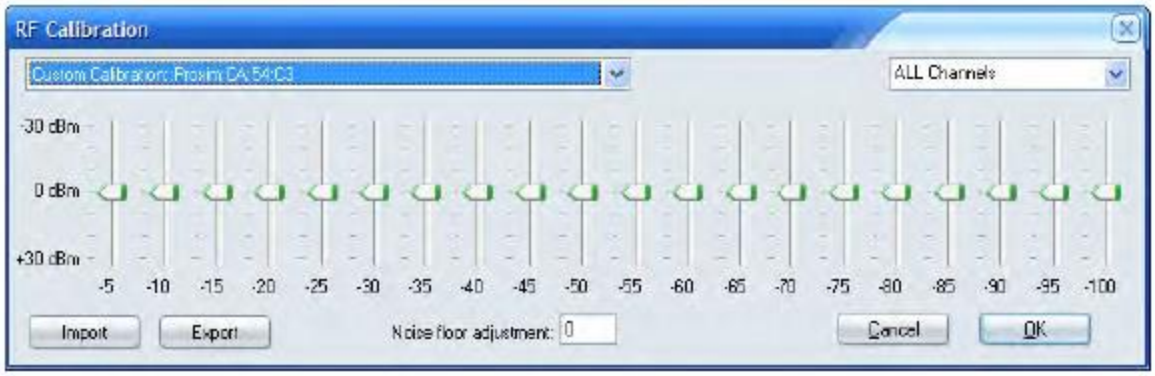
Шаблоны пользовательской калибровки создаются для выравнивания показаний мощности сигнала между любой комбинацией адаптеров Wi-Fi. Начните с измерения (аналогично процессу, описанному в разделе предварительной калибровки) двух разных радиомодулей со смещением нуля на разных расстояниях, сравнивая уровни принимаемого сигнала на каждом из них. Затем рассчитайте разницу между адаптерами Wi-Fi и используйте ее для установки смещения одного радиомодуля, чтобы он соответствовал показаниям мощности сигнала другого адаптера Wi-Fi.

Данная функция позволяет откалибровать мощность радиосигнала и уровень собственных шумов беспроводной сетевой карты с шагом 5 дБм. Это даст возможность нормализовать разные адаптеры Wi-Fi, чтобы они показывали одинаковые значения уровня сигнала. Без использования этой функции показания уровней сигнала между адаптерами Wi-Fi от разных производителей или даже между разными моделями одного и того же производителя могут значительно отличаться.

Значения по горизонтали (от -5 до -100) представляют уровни мощности сигнала, принимаемого адаптером Wi-Fi. Для каждого уровня мощности сигнала можно установить смещение (от -30 дБ до + 30 дБ), перемещая ползунки вверх или вниз.

Для настройки мощности радиочастотного сигнала адаптера беспроводной сети сделайте следующее:

1. В разворачивающемся списке выберите Custom Calibration (Пользовательская калибровка) (если беспроводный сетевой адаптер не был предварительно откалиброван, здесь необходимо добавить его имя). Смотрите рисунок ниже.



2. Щелкните кнопкой мыши на направленной вниз стрелке в правом верхнем углу и выберите нужный канал.

Примечание: Обычно радиочастотная калибровка выполняется для каждого канала отдельно, если только не нужно применить одну и ту же калибровку ко всем каналам. В этом случае в меню списка каналов следует выбрать All Channels (Все каналы).

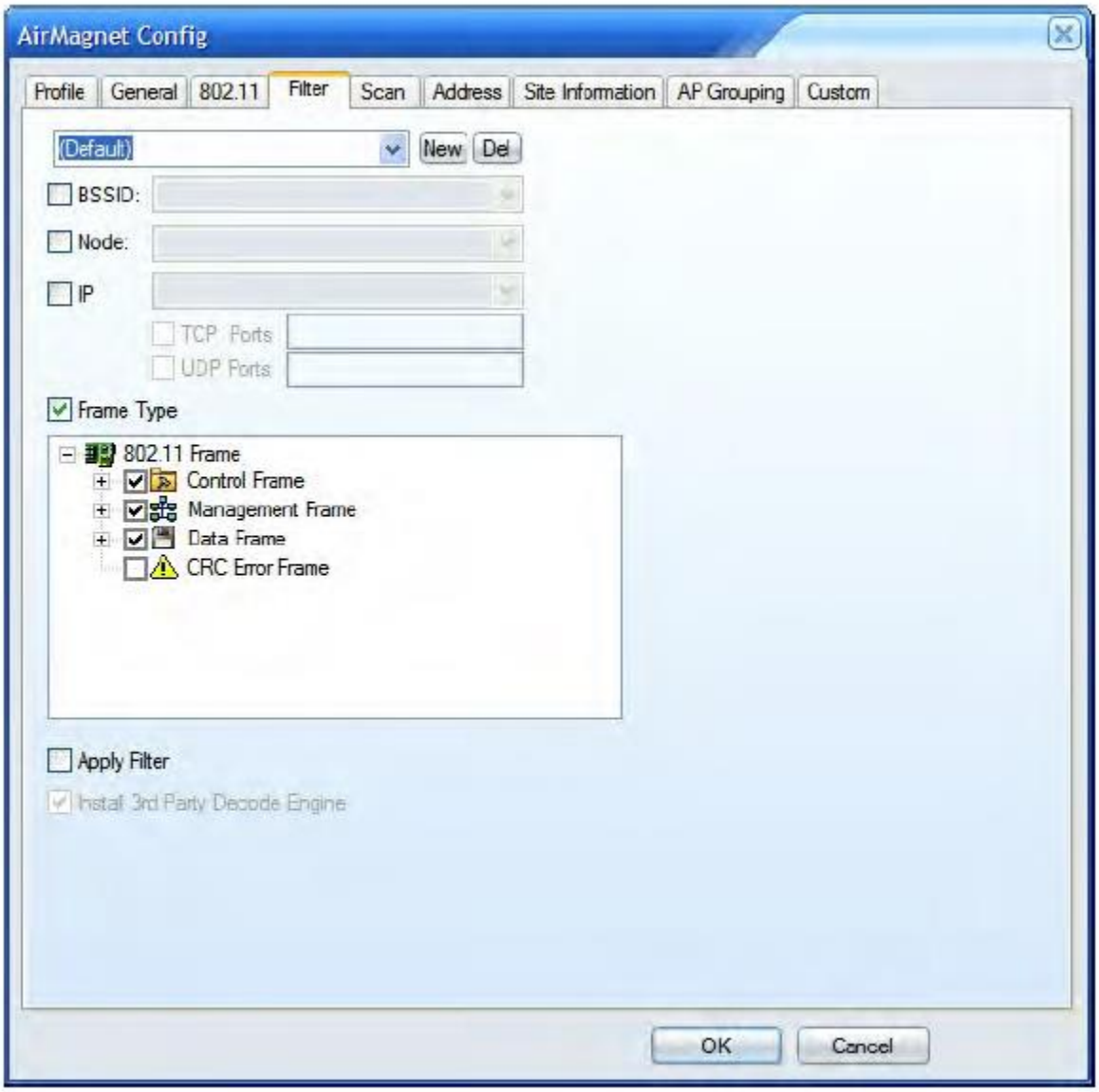
3. Для регулировки мощности радиочастотного сигнала используйте ползунки.
4. При желании выделите значение в поле регулировки уровня собственных шумов и введите новое значение уровня.
5. По завершении нажмите кнопку OK.

Настройка фильтров данных

Приложение AirMagnet WiFi Analyzer предоставляет четыре варианта фильтрации захватываемых данных, по идентификатору BSSID, узлу (Node), IP-адресу (IP) и/или типу кадра (Frame Type). Они позволяют пользователю использовать для проведения статистического анализа различные технологии выборки для сканирования всех доступных каналов на наличие кадров 802.11. По умолчанию приложение AirMagnet WiFi Analyzer захватывает все данные, которые проходят через сеть WLAN, и отображает их на экране. Иногда это может затруднить выявление и решение проблем, которые являются наиболее важными для сетей пользователей.

Для быстрого поиска и устранения сложных проблем протокола сначала необходимо сузить сканирование до определенного идентификатора SSID или точки доступа и связанного канала. После этого следует использовать различные опции фильтрации в AirMagnet WiFi Analyzer, чтобы отфильтровать или отбросить нежелательные пакеты 802.11. Такие базовые методы поиска и устранения неисправностей помогут обнаружить и выявить любую существующую проблему.

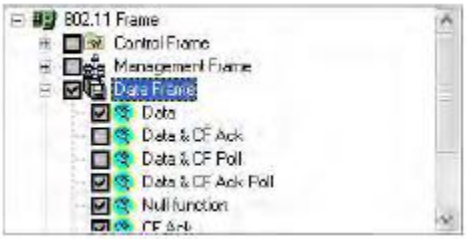
Создание нового фильтра



1. На экране AirMagnet Configuration (Конфигурация AirMagnet) откройте вкладку Filter (Фильтр).
2. В диалоговом окне Filter (Фильтр) нажмите New (Создать) и введите имя фильтра.
3. По очереди настройте параметры SSID, Node, IP или Frame Type.

- Для фильтрации по идентификатору BSSID поставьте метку в поле BSSID и выберите BSSID из разворачивающегося списка.
- Для фильтрации по узлу поставьте метку в поле Node и выберите узел из разворачивающегося списка.

- Для фильтрации по IP-адресу поставьте метку в поле IP, выберите IP-адрес из разворачивающегося списка, отметьте TCP и/или UDP и введите номер (номера) порта.
- Для фильтрации по типу кадра поставьте метку в поле Frame Type, по очереди разверните параметры кадра, снимите метки со всех типов кадров, а затем выберите только те из них, которые вам интересны.



4. Установите метку в поле Apply Filter (Применить фильтр). Для активации фильтра в этом поле обязательно должна стоять метка.
5. Нажмите кнопку OK.

Примечание: Когда в поле Apply Filter (Применить фильтр) устанавливается метка, выбранный в этом диалоговом окне фильтр будет автоматически применяться на экране Decodes (Декодирование), то есть через фильтр будут проходить только кадры, соответствующие его параметрам. Все созданные пользователем фильтры будут храниться в разворачивающемся списке в верхней части диалогового окна Filter (Фильтр). Для использования просто выберите любой из них.

Удаление существующего фильтра

По мере создания все большего количества фильтров разворачивающийся список Filter (Фильтр) может переполниться. Для эффективной работы можно удалить фильтры, которые больше не используются.

Чтобы удалить фильтр:
1. В диалоговом окне AirMagnet Configuration > Filter (Конфигурация > Фильтр) щелкните кнопкой мыши на разворачивающемся списке и выделите фильтр, который нужно удалить.
2. Нажмите Del (Удалить).
3. Нажмите кнопку OK.

Установка стороннего декодера

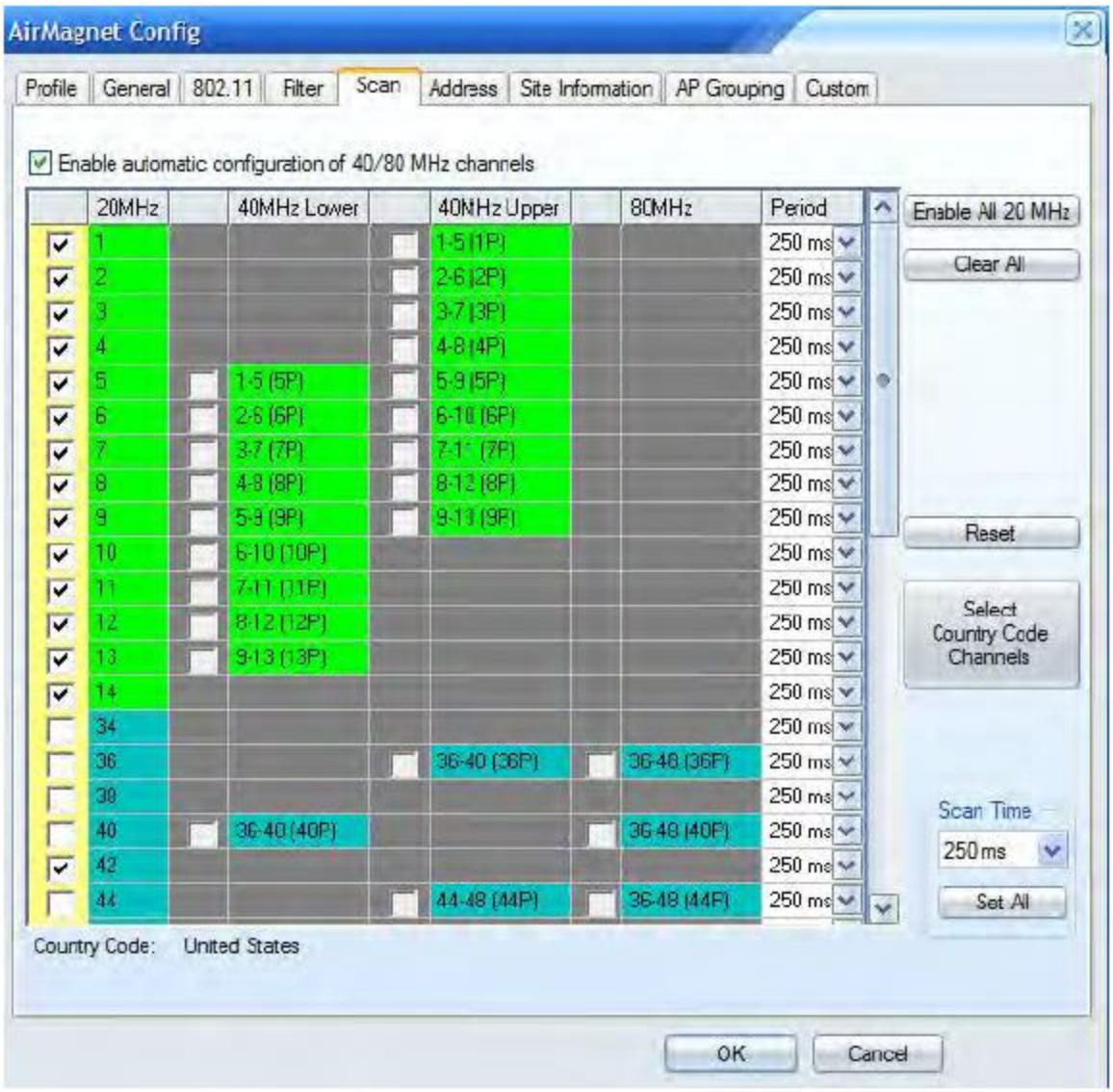
Если во время установки приложения не была выбрана установка сторонних декодеров (3rd Party Decodes), это можно сделать здесь. Данная функция позволит декодировать верхние уровни ваших файлов захвата.

Чтобы установить сторонний декодер:
1. Поставьте метку в поле 3rd Party Decodes Engine (Сторонний декодер). После этого начнется установка.
2. Примите условия лицензии GNU. Обратитесь к разделу «Лицензия на декодеры сторонних производителей».
3. Также можно разрешить доступ к этой функции всем, кто использует данный компьютер.

Настройка сканирования каналов

Данная опция позволяет пользователю выбрать канал или каналы, которые приложение AirMagnet WiFi Analyzer будет сканировать, а также установить частоту, на которой это сканирование будет осуществляться.

Примечание: Доступные опции могут различаться в зависимости от используемого адаптера Wi-Fi (например, 802.11n или 802.11ac).



Радиочастоты (каналы) и мощность излучения для стандартов 802.11 определяются нормативными правилами. Чтобы соответствовать этим нормативным требованиям, устройства WLAN в разных странах мира предварительно настроены для работы на разных каналах. В следующей таблице приведены данные о распределении каналов в основных частях мира.

Регион/Страна	802.11b/g	802.11a/ac
Америка	1 ~ 11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 132, 136, 149, 153, 157, 161
Большая часть Европы и Австралия	1 ~ 13	36, 40, 44, 48, 52, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Франция	10 ~ 14	36, 40 44, 48, 52, 56, 60, 64
Испания	10 ~ 11	36, 40 44, 48, 52, 56, 60, 64
Япония	1 ~ 14	36, 40, 44, 48, 52, 56, 60, 64
Тихоокеанский регион (Китай, Тайвань, Гонконг, Сингапур, Корея)	1 ~ 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

Несмотря на эти нормативные требования, бывают случаи, когда из-за неправильной настройки конфигурации или наличия злонамеренной неавторизованной точки доступа запрещенные каналы содержат действующие устройства 802.11. Поскольку при сканировании приложением AirMagnet не излучаются радиоволны, оно полностью соответствует всем нормативным требованиям.

Использование во время работы всемирного режима дает три преимущества:

1. Для администраторов WLAN и консультантов, которые путешествуют по всему миру, функция всемирного режима AirMagnet позволяет легко осуществлять выбор между регулируемыми каналами.

2. Поскольку неавторизованные точки доступа могут работать на любом канале независимо от нормативных требований, возможность сканирования всех каналов на наличие подобных точек доступа имеет важное значение.
3. Также дополнительным преимуществом является возможность обнаружения неправильно настроенных устройств WLAN, работающих с нарушением нормативных правил.

Для настройки параметров сканирования каналов:

1. В диалоговом окне AirMagnet Configuration (Конфигурация AirMagnet) откройте вкладку Scan (Сканирование).

Примечание: По умолчанию выбраны все каналы 20 МГц.

2. Чтобы удалить настройки сканирования по умолчанию нажмите Clear All (Очистить все), затем выберите только тот канал или каналы, которые хотите просканировать.
3. Нажатие Country Code (Код страны) позволяет выбрать поддерживаемые каналы диапазона 5 ГГц в соответствии с настройкой Country (Страна) на вкладке 802.11.
4. Щелкните кнопкой мыши в соответствующем поле в столбце Period (ms) (Период (мс)) для каждого канала, и в разворачивающемся списке выберите частоту сканирования канала.
5. При необходимости щелкните кнопкой мыши на направленной вниз стрелке под Scan Time (Время сканирования) (в правом нижнем углу диалогового окна), выберите опцию в разворачивающемся списке, а затем нажмите Set All (Установить все), чтобы изменить время сканирования всех каналов на выбранное значение.
6. Если необходимо восстановить настройки сканирования по умолчанию, нажмите Reset (Сброс).
7. Нажмите кнопку ОК.

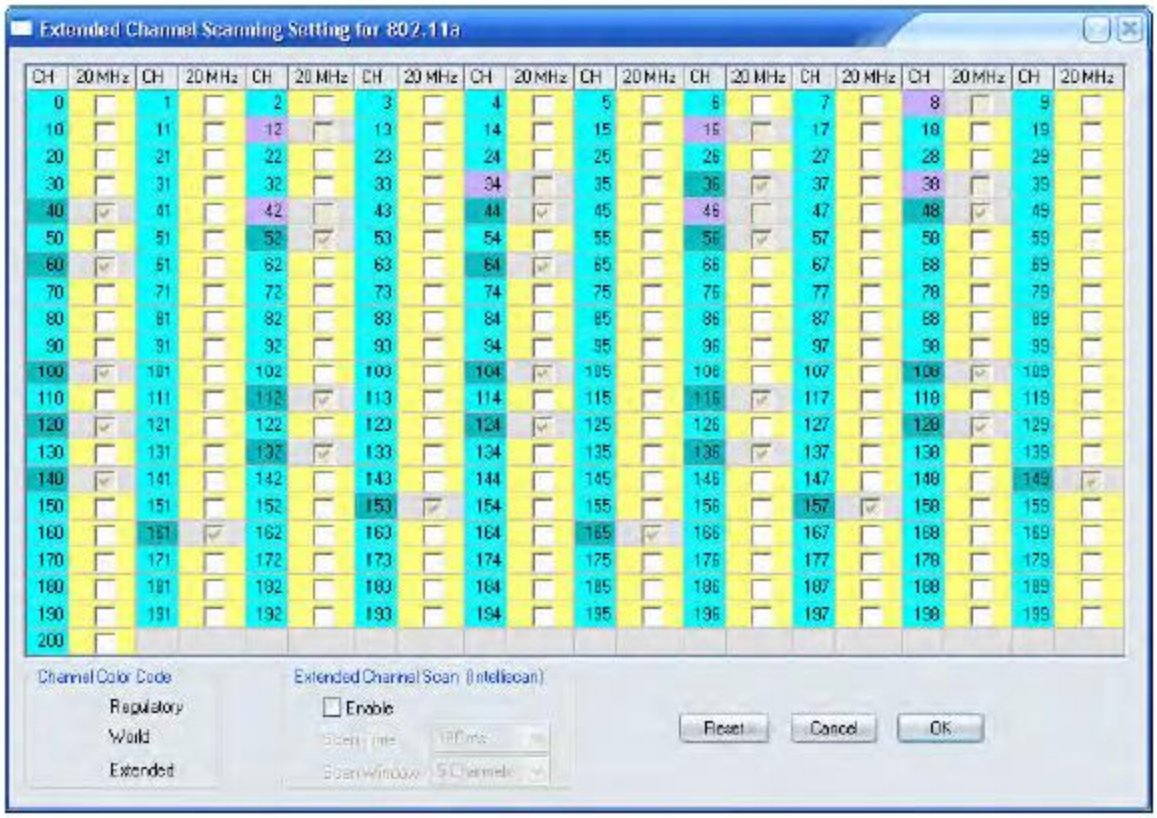
Примечание: Поле Enable automatic configuration of 40 MHz channels (802.11n) or 40/80 MHz channels (802.11ac) (Включить автоматическую настройку каналов 40 МГц (802.11n) или каналов 40/80 МГц (802.11ac)) отмечено по умолчанию.

Настройка сканирования каналов для нескольких адаптеров

Чтобы пользователи могли указывать индивидуальные параметры сканирования каналов для каждого отдельного используемого адаптера, вкладка Scan (Сканирование) в меню конфигурации приложения AirMagnet WiFi Analyzer была немного изменена.

Как показано выше, разворачивающиеся меню выбора индивидуальных каналов предусмотрены для каждого адаптера, который активно захватывает данные в приложении. Просто укажите желаемый канал для каждого адаптера и нажмите кнопку OK для настройки параметров сканирования.

Сканирование расширенных каналов 802.11a



Расширенные каналы относятся к тем каналам 802.11a, которые обычно не используются большинством компаний или стран. Нажав кнопку Select Country Code Channels (Выбрать каналы по коду страны), можно сканировать только стандартные для стран каналы. Однако, поскольку для хакерских атак и атак от внешних источников не всегда выбираются обычные каналы, можно, нажав кнопку Extended… (Расширенные), просканировать расширенные каналы, которые обычно не используются. Некоторые устройства также используют расширенные каналы по умолчанию (или специально настроены для этого); настройка приложения AirMagnet Wi-Fi Analyzer на сканирование этих каналов поможет убедиться, что все устройства в вашей сети настроены должным образом в соответствии с политиками вашей компании.

Для сканирования 802.11a можно настроить любое количество каналов. Приложение AirMagnet Wi-Fi Analyzer будет включать выбранные здесь каналы в процесс сканирования вместе со стандартными каналами. Кроме того, для настройки того, как приложение AirMagnet Wi-Fi Analyzer будет сканировать каналы, которые вы также не проверяете, можно использовать инструменты внизу экрана.

Во время обычного сканирования приложение AirMagnet Wi-Fi Analyzer просканирует стандартные каналы и выбранные расширенные каналы. Затем оно просканирует ряд каналов 802.11a, которые не выбраны. Для управления этим используются параметры Scan Time (Время сканирования) и Scan Window (Окно сканирования) внизу. Время сканирования определяет количество времени, затрачиваемое на сканирование, а окно – количество одновременно сканируемых каналов. После сканирования указанного окна каналов приложение AirMagnet Wi-Fi Analyzer повторно просканирует стандартные каналы, а затем продолжит работу с расширенными каналами.

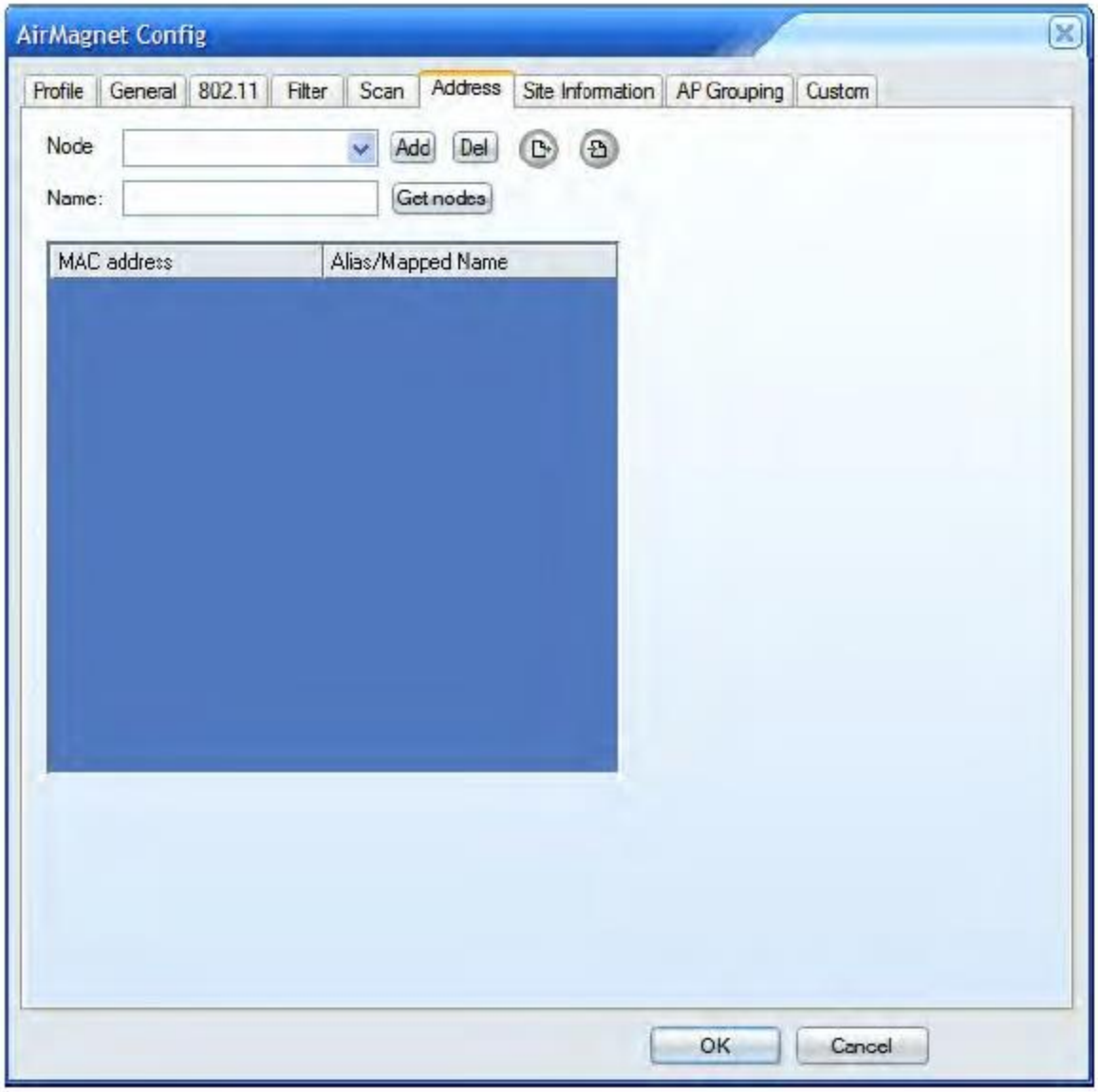
Карта Intel 2915ABG не поддерживает сканирование расширенных каналов 802.11a.

Настройка адресной книги системы

Приложение AirMagnet WiFi Analyzer фиксирует MAC-адреса всех беспроводных устройств, обнаруженных в сети с момента включения, и сохраняет эти данные в своей внутренней базе данных. Создание адресной книги позволяет присвоить MAC-адресу каждого беспроводного устройства псевдоним для более легкого запоминания и управления активами беспроводной локальной сети.

Создание адресной книги

Создание адресной книги включает добавление MAC-адресов устройств и ввод псевдонима для каждого из них.



Для создания адресной книги:

1. В диалоговом окне AirMagnet Configuration (Конфигурация AirMagnet) откройте вкладку Address (Адрес).
2. Щелкните кнопкой мыши на направленной вниз стрелке рядом с полем Node (Узел) и выберите MAC-адрес в разворачивающемся списке.
3. Щелкните кнопкой мыши на поле Name (Имя) и введите псевдоним для MAC-адреса.
4. Нажмите Add (Добавить). Вновь созданная пара «MAC-адрес – псевдоним» появится в таблице адресов ниже.
5. Для добавления новых записей в адресную книгу повторяйте шаги 2 – 4.

Создание адресной книги с помощью кнопки Get Nodes (Получить узлы)

Кроме того, для автоматического заполнения адресной книги всеми MAC-адресами, захваченными с момента включения приложения AirMagnet WiFi Analyzer, можно нажать кнопку Get nodes (Получить узлы). После заполнения книги можно будет присвоить записям псевдонимы.

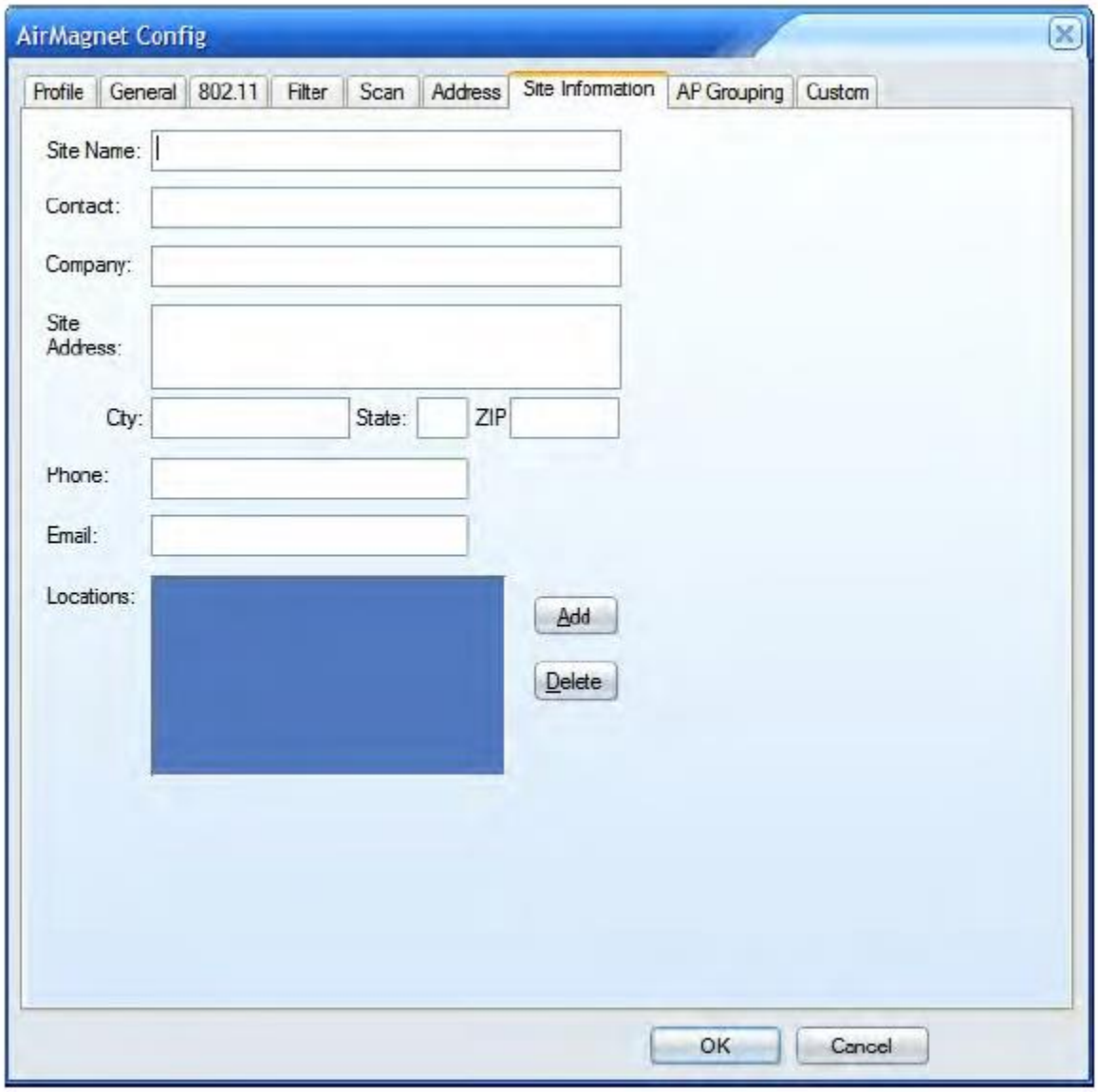
1. На экране AirMagnet Config > Address (Конфигурация AirMagnet > Адрес) нажмите Get nodes (Получить узлы). Столбец MAC-адресов в адресной таблице будет заполнен MAC-адресами, захваченными приложением AirMagnet.
2. Щелкните кнопкой мыши на столбце Mapped Name (Соответствующее имя) и введите псевдоним, соответствующий MAC-адресу слева.
3. Чтобы добавить дополнительные псевдонимы, повторяйте шаг 2.
4. По завершении нажмите кнопку OK.

Удаление записей из адресной книги

Запись из адресной книги можно удалить (удаляется MAC-адрес или пара «MAC-адрес – псевдоним»).
Для удаления записи из адресной книги:
1. Выделите запись, которую хотите удалить.
2. Нажмите Delete (Удалить).
3. Нажмите OK.

Указание информации об объекте

После настройки всех системных параметров можно также добавить в профиль некоторую информацию, относящуюся к конкретному объекту. Это связано с тем, что приложение AirMagnet Wi-Fi Analyzer является мобильным инструментом обеспечения безопасности беспроводной сети, который можно переносить в разные беспроводные локальные сети или в разные части одной и той же беспроводной локальной сети. Поскольку сетевая инфраструктура разных объектов или разных частей одной сети может отличаться, удобно включать в профили некоторую информацию по конкретному объекту. Это облегчит архивирование обследований площадки и/или системных профилей.



Для добавления в профиль информации о площадке:

1. В диалоговом окне AirMagnet Configuration (Конфигурация AirMagnet) откройте вкладку Site Information (Информация об объекте).
2. Заполните форму, указав всю необходимую информацию.
3. Нажмите Add (Добавить). В поле Location (Местоположение) появится запись «Location 1».
4. Нажмите кнопку OK.

Группирование точек доступа

Настройка группирования точек доступа

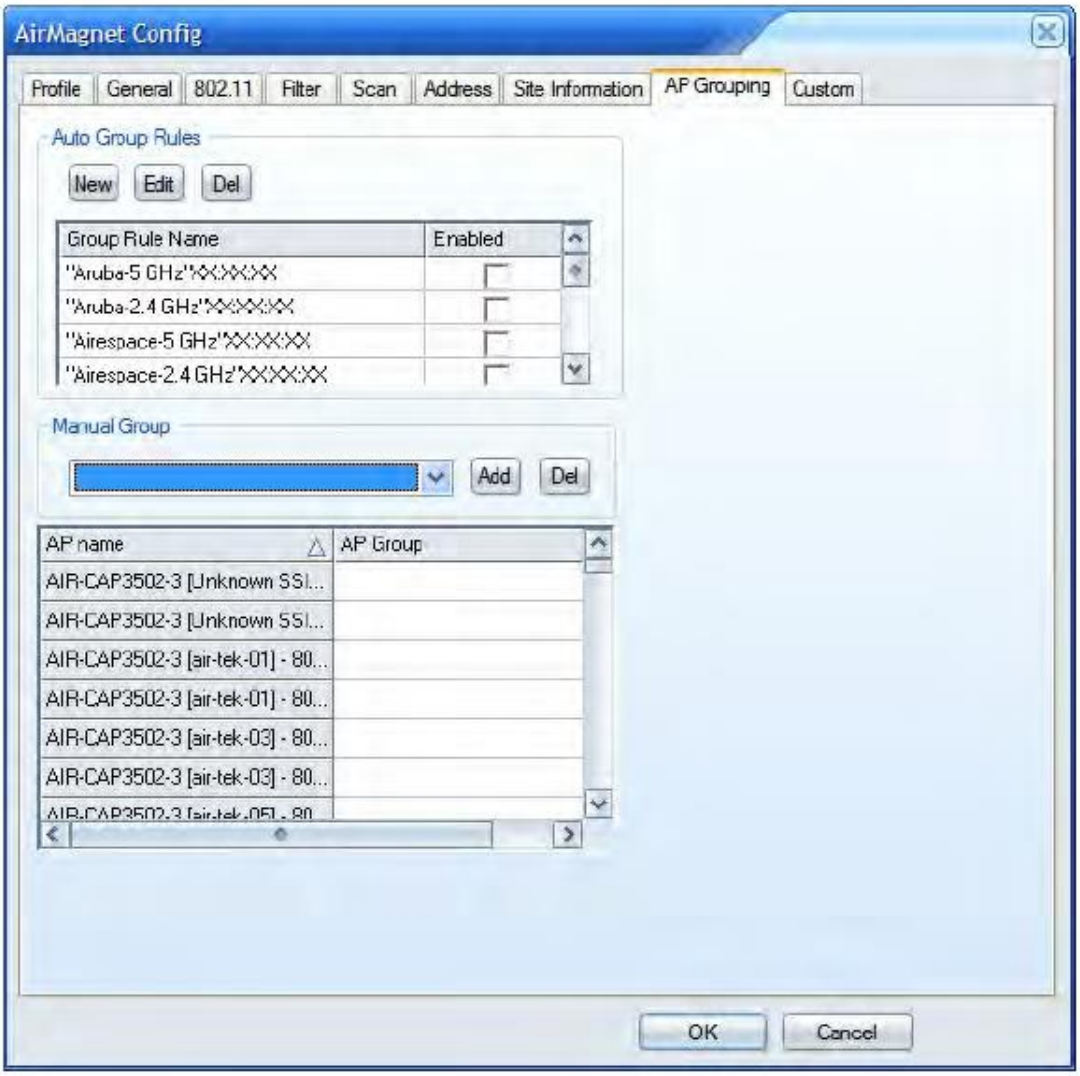
Вкладка AP Grouping (Группирование точек доступа) позволяет ввести имена для отдельных устройств, которые используют несколько VLAN под разными идентификаторами SSID. Это затрагивает многие страницы, где отдельные SSID будут отображаться и выглядеть как разные устройства, хотя на самом деле они принадлежат одному и тому же объекту. Функция группирования точек доступа предоставит возможность увидеть, что эти, казалось бы, разные устройства принадлежат одной и той же сети VLAN.

Группирование точек доступа можно настроить одним или всеми из следующих способов:

- Использование правил по умолчанию для автоматического группирования точек доступа.
- Группирование точек доступа с помощью правил автоматического группирования точек доступа.
- Создание групп точек доступа вручную.

Создание правил автоматического группирования точек доступа

Приложение AirMagnet WiFi Analyzer имеет несколько встроенных правил «автоматического» группирования точек доступа. После включения эти правила позволят приложению AirMagnet WiFi Analyzer автоматически объединять в одну группу точек доступа все устройства, соответствующие указанным в конкретном правиле группирования точек доступа критериям. Это особенно удобно, если организация использует устройства определенного производителя; приложение AirMagnet WiFi Analyzer сможет распознавать эти устройства среди всех обнаруженных им устройств и группировать соответствующим образом.



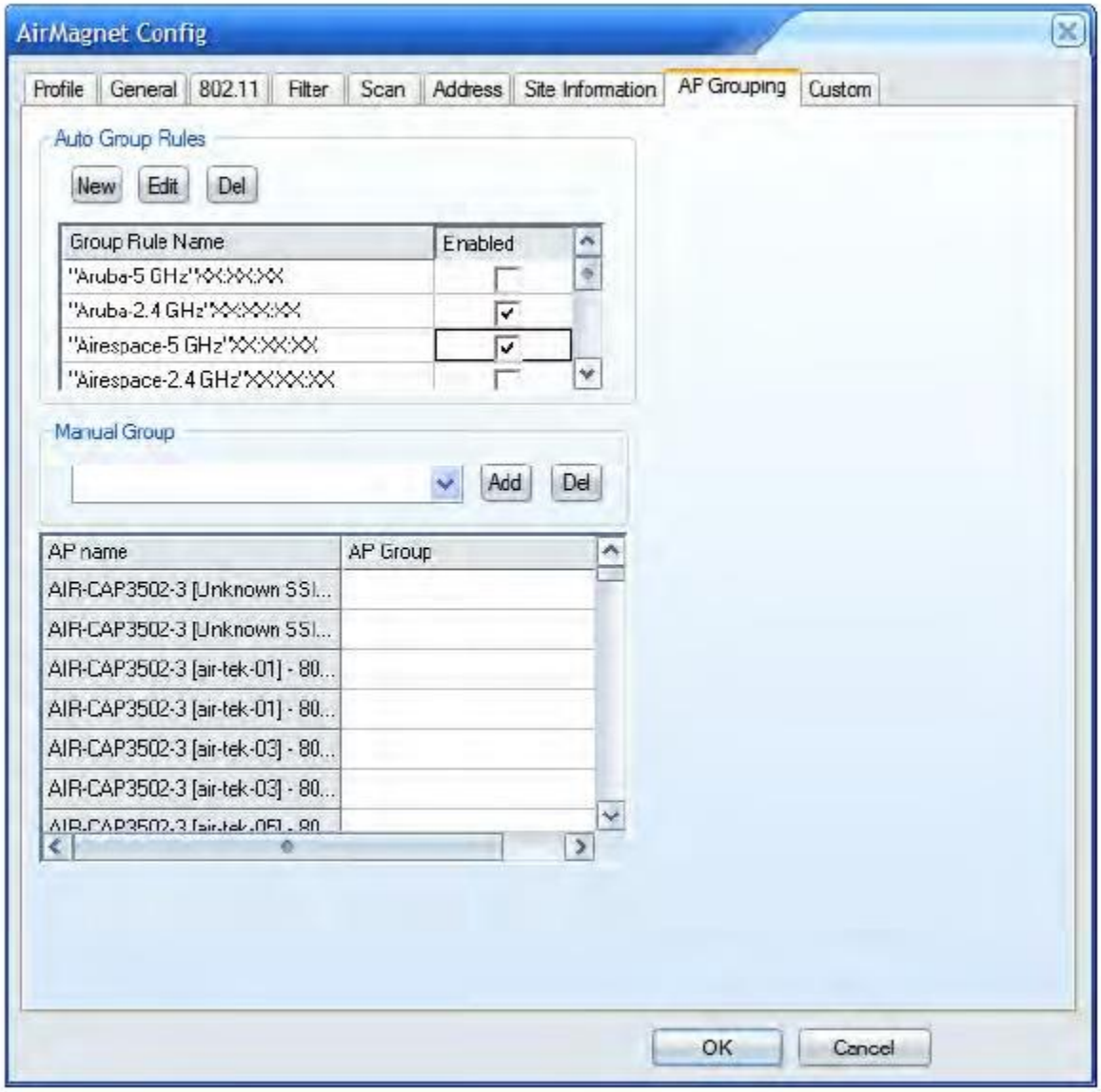
Для настройки группирования точек доступа:

1. В диалоговом окне AirMagnet Configuration (Конфигурация AirMagnet) откройте вкладку AP Grouping (Группирование точек доступа).
2. Нажмите New (Создать). Появится диалоговое окно Auto Group AP Rule (Правило автоматического группирования точек доступа).
3. Введите информацию и/или сделайте выбор, как описано в таблице ниже.
4. Нажмите кнопку OK.

Ввод/Выбор	Описание
Vendor ID (Идентификатор производителя)	Укажите идентификатор производителя устройств, на которые распространяется правило автоматического группирования точек доступа.
Band (Диапазон)	Укажите тип среды, используемой устройствами.
MAC address last hex-digit starting (Начиная с последней шестнадцатеричной цифры MAC-адреса)	Выберите последнюю шестнадцатеричную цифру MAC-адресов, с которой должно начинаться правило автоматического группирования точек доступа.
Number of contiguous MAC address (Количество последовательных MAC-адресов)	Позволяет выбрать количество последовательных MAC-адресов, которые необходимо классифицировать в группе.
Ascending (По возрастанию)	Если выбрано, правило будет вести прямой отсчет до указанного максимального значения.
Descending (По убыванию)	Если выбрано, правило будет вести обратный отсчет до указанного максимального значения.

Применение правил автоматического группирования точек доступа

Приложение AirMagnet WiFi Analyzer поставляется с несколькими встроенными правилами «автоматического» группирования точек доступа, которые облегчают пользователю использование этой мощной функции управления. Эти правила автоматического группирования точек доступа по умолчанию, а также все настраиваемые правила, созданные пользователем, отображаются в разделе Auto Group Rules (Правила автоматического группирования) диалогового окна AP Grouping (Группирование точек доступа). После включения эти правила позволят приложению AirMagnet WiFi Analyzer автоматически объединять все устройства, соответствующие указанным в конкретном правиле группирования точек доступа критериям, в одну группу точек доступа. Это особенно удобно, если организация использует устройства определенного производителя; приложение AirMagnet WiFi Analyzer сможет распознавать эти устройства и группировать соответствующим образом.



Для активации правил автоматического группирования точек доступа

1. В разделе Auto Group Rules (Правила автоматического группирования) выберите правила, поставив метки в соответствующих полях.
2. Нажмите кнопку OK.

Создание групп точек доступа вручную

Также приложение AirMagnet WiFi Analyzer предоставляет пользователям возможность создавать группы точек доступа, используя любую подходящую систему именования. После настройки групп, всё, что нужно сделать, так это поочередно вручную назначить точки доступа группам. Это не только дает свободу и гибкость в именовании наших групп или групп точек доступа, но также позволяет точно знать, какие точки доступа помещены в каждую из групп.

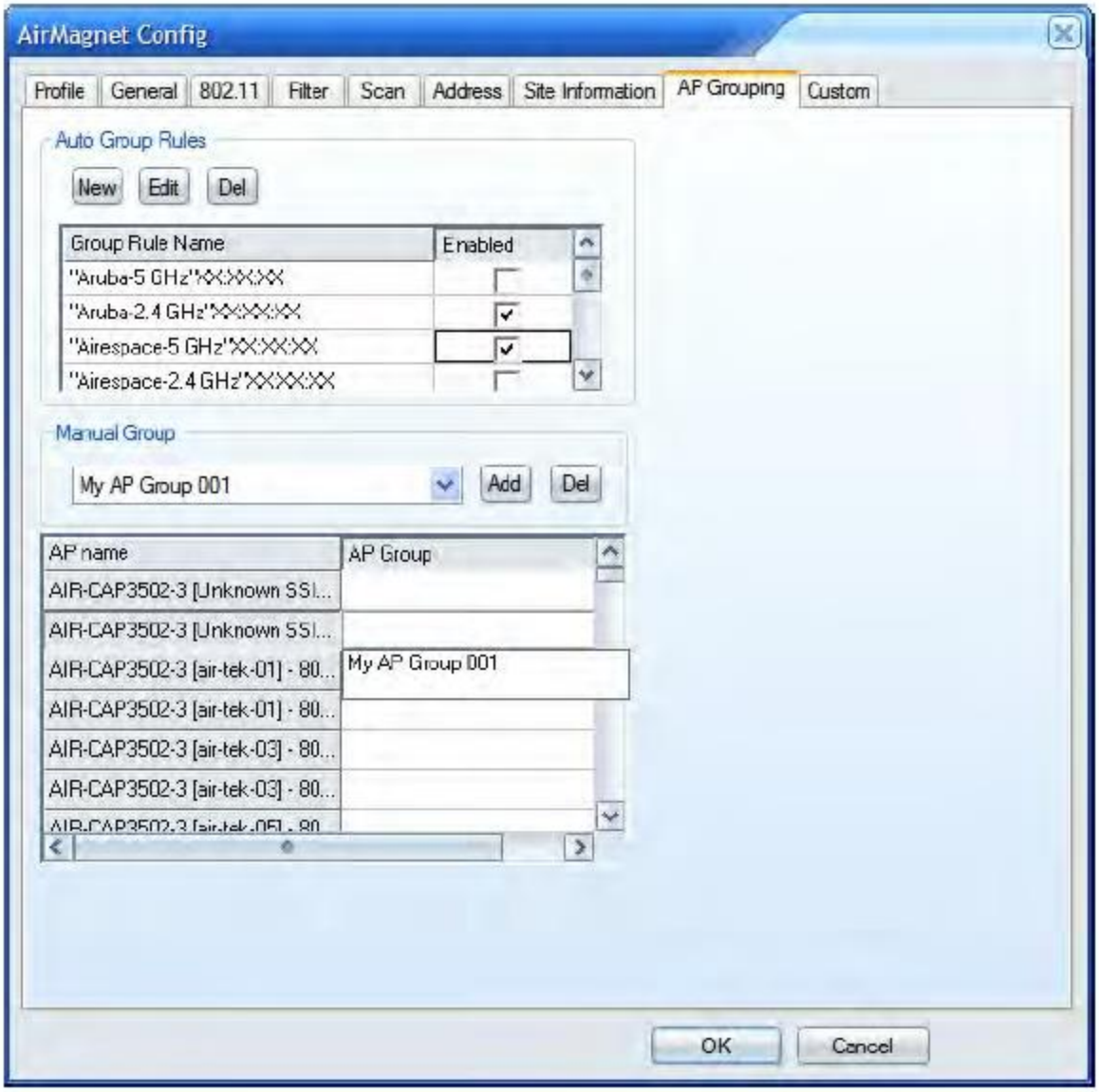
Чтобы создать группы точек доступа вручную:

1. В разделе Manual Group (Группирование вручную) диалогового окна AP Grouping (Группирование точек доступа) нажмите Add (Добавить). Откроется диалоговое окно Manual Group (Группирование вручную).

2. Введите имя создаваемой группы точек доступа и нажмите кнопку OK.
3. Для создания необходимого числа групп точек доступа повторяйте шаги 1 и 2.

Примечание: Имена созданных групп точек доступа появятся в столбце AP Group Name (Имя группы точек доступа) в разделе Manual Group (Группирование вручную) при щелчке кнопкой мыши на этом столбце.

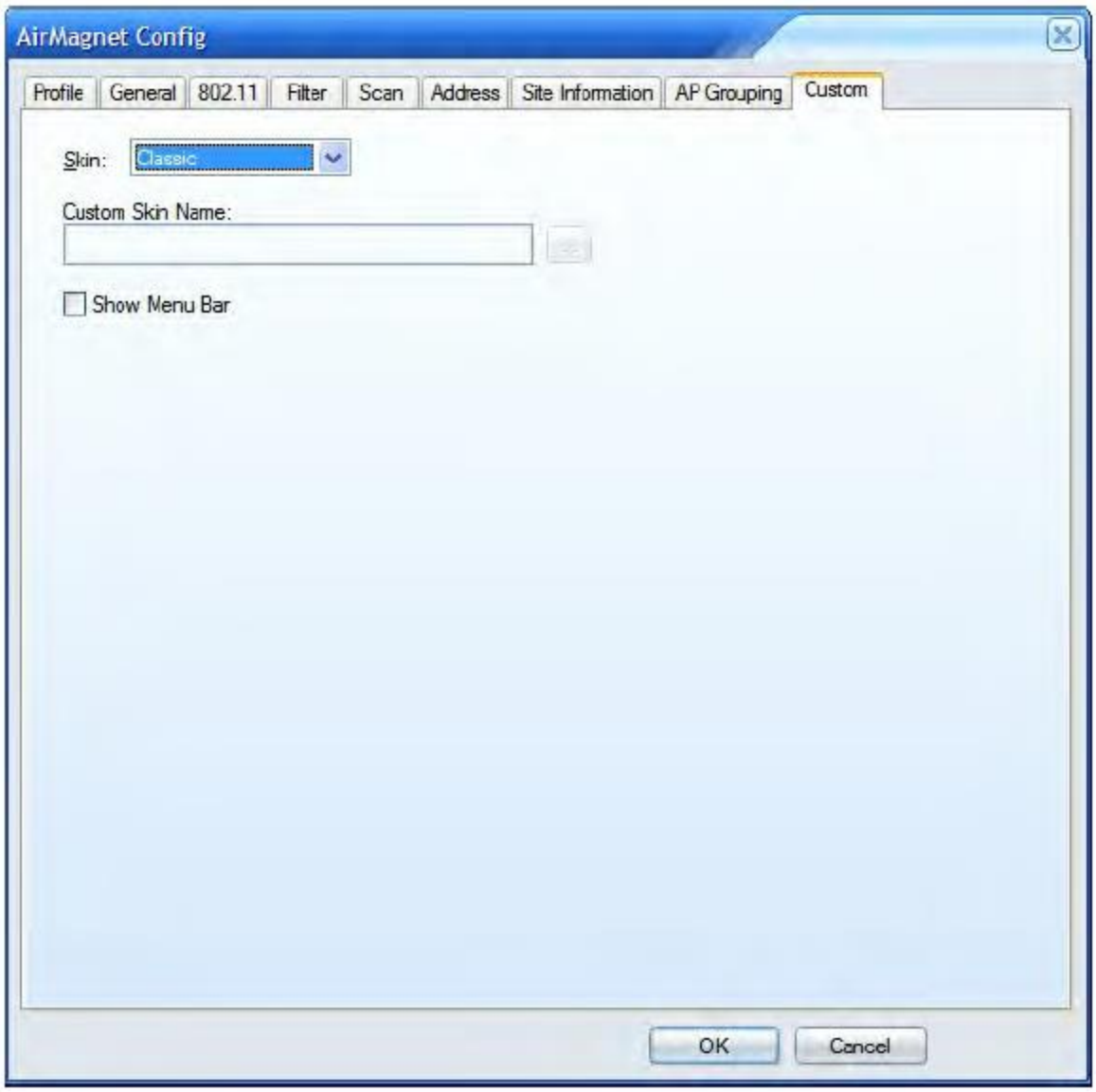
4. Назначьте точки доступа группам, щелкнув кнопкой мыши на столбце AP Group (Группа точек доступа) и выбрав нужную группу точек доступа.



5. Повторяйте шаг 4, пока не будут назначены все точки доступа.
6. Нажмите кнопку OK.

Настройка пользовательского интерфейса

Вкладка Custom содержит несколько опций, позволяющих пользователю выбрать или изменить внешний вид (цветовую схему) приложения AirMagnet WiFi Analyzer.



Чтобы выбрать или изменить цвет оболочки пользовательского интерфейса:

1. В диалоговом окне AirMagnet Configuration (Конфигурация AirMagnet) откройте вкладку Custom (Пользовательская настройка).
2. Щелкните кнопкой мыши на направленной вниз стрелке Skin (Оболочка) и выберите в разворачивающемся списке один из вариантов.
3. Если вы хотите, чтобы в верхней части экрана отображалась панель меню, поставьте метку в поле Show Menu Bar (Показывать панель меню).
4. Нажмите кнопку OK.

Примечание: В описанной выше процедуре показано, как выбрать или изменить цвет оболочки пользовательского интерфейса приложения AirMagnet WiFi Analyzer среди опций по умолчанию. Также вы можете использовать свои собственные оболочки. Все, что нужно сделать, так это нажать квадратную кнопку (Browse) и перейти к месту, где находится файл пользовательской оболочки. Файлы оболочек должны иметь формат .msstyle; их можно загрузить из различных источников в сети Интернет.

Поле	Описание
Skin (Оболочка)	Разворачивающийся список Skin (Оболочка) позволяет выбрать одну из трех предварительно настроенных оболочек. Кроме того, можете выбрать опцию Custom (Пользовательская) и использовать свою собственную оболочку, как описано ниже.
Custom Skin Name (Имя пользовательской оболочки)	Если в разворачивающемся списке оболочек выбрана опция Custom (Пользовательская), можете нажать кнопку Browse и перейти к месту, где были сохранены пользовательские оболочки. Файлы оболочек должны иметь формат .msstyle; их можно загрузить из различных источников в сети Интернет.
Show Menu Bar (Показывать панель меню)	Если в данном поле стоит метка, в верхней части экрана приложения будут отображаться меню File (Файл), Tools (Инструменты) и Help (Справка). Эти меню выполняют многие из тех задач, что и кнопки на панели инструментов.

Подключение к удаленной системе

Для удаленного поиска и устранения неисправностей приложение AirMagnet WiFi Analyzer позволяет подключаться к удаленным системам.

Примечание: Подключение к удаленной системе не поддерживается в среде NAT (Трансляция сетевых адресов).

Режим удаленной работы приложения AirMagnet Wi-Fi Analyzer

Компьютер с запущенным приложением AirMagnet WiFi Pro можно перевести в режим удаленной работы. Когда компьютер установлен в этот режим, к нему можно установить удаленное подключение с локального компьютера, на котором запущено приложение AirMagnet WiFi Analyzer Pro. Локальный компьютер переключится на удаленный адаптер для сбора данных.

Сначала установите удаленный компьютер в режим удаленной работы:
1. В меню File (Файл) выберите Operation Mode (Режим работы).
2. Выберите AirMagnet Remote WiFi Analyzer mode (Режим удаленного анализатора WiFi).
3. Установите пароль (Password), который будет использоваться позднее для подключения к этому удаленному компьютеру.
4. Определите IP-адрес компьютера.

На локальном компьютере подключитесь к удаленному компьютеру:
1. В меню File (Файл) выберите Connect to (Подключиться к).
2. Выберите AirMagnet Remote WiFi Analyzer.
3. В поле Laptop/PC IP (IP-адрес ноутбука/ПК) введите IP-адрес удаленного компьютера.
4. В поле User Name (Имя пользователя) введите AirMagnetSensor.
5. В поле Password (Пароль) введите пароль, созданный в диалоговом окне Remote Operation Mode (Режим удаленной работы).

Подключение к датчику AirMagnet SmartEdge

К некоторым моделям датчика AirMagnet SmartEdge можно подключаться удаленно.

Примечание: В этом разделе описывается настройка нового датчика AirMagnet SmartEdge. Попытка изменить конфигурацию существующего датчика AirMagnet SmartEdge не поддерживается. С любыми вопросами обращайтесь к торговому представителю AirMagnet или в службу технической поддержки.

Модель датчика	Описание
AM/A5200	ДАТЧИК AIRMAGNET, A/B/G/N, ВНЕШНЯЯ АНТЕННА
AM/A5205	ДАТЧИК AIRMAGNET, A/B/G/N, ВНУТРЕННЯЯ АНТЕННА
AM/A5220	ДАТЧИК AIRMAGNET SPECTRUM, A/B/G/N, ВНЕШНЯЯ АНТЕННА
AM/A5225	ДАТЧИК AIRMAGNET SPECTRUM, A/B/G/N, ВНУТРЕННЯЯ АНТЕННА

Датчик должен быть настроен для использования с приложением AirMagnet WiFi Analyzer Pro.

Настройка датчика AirMagnet SmartEdge

1. Включите датчик AirMagnet SmartEdge (адаптер PoE, совместимый с 802.3af, или адаптер 12 В).
2. Соедините последовательный консольный порт на датчике AirMagnet SmartEdge с последовательным портом компьютера входящим в комплект последовательным кабелем.
3. Потребуется запустить эмулятор терминала. (Из сети Интернет можно скачать бесплатные или платные программы-эмуляторы терминала, например, «PuTTY» или «SecureCRT»).
4. Выберите COM-порт, к которому подключен датчик AirMagnet SmartEdge. По умолчанию - COM1.
5. Сделайте следующие записи или выбор для сеанса терминала:

Параметр	Настройка
Бит в секунду	115200
Бит данных	8
Проверка четности	Нет
Стоповый бит	1
Управление потоком	Нет

6. Продолжая сеанс терминала, в ответ на приглашение нажмите Enter.
7. Будет предложено ввести Shared Secret Key (Общий секретный ключ). Ключ по умолчанию - «airmagnet».

После каждой из следующих настроек конфигурации будет предложено перезагрузить компьютер. Если не указано иное, выбирайте «Нет» (N) до завершения настройки конфигурации, затем перезагрузите компьютер.
(Чтобы получить список параметров конфигурации, введите: config > help).

8. Введите: config> set enterprise enable.
   Данная команда настраивает датчик для использования с приложением AirMagnet WiFi Analyzer.
9. Когда будет предложено перезагрузить датчик, выберите «Да» (Y). После перезагрузки датчика продолжите настройку.
10. Введите: config > set sensor.
    Эта команда устанавливает имя и «общий секретный ключ» для датчика SmartEdge (в имени не допускаются пробелы).
11. Введите: config > set network.
    Эта команда устанавливает параметры IP-адреса (IP-адрес, маску подсети и шлюз по умолчанию), например:
    DHCP Enabled (Y/N)? Y (DHCP включен (Да/Нет)? Да)
    Obtain DNS server addresses automatically (Y/N)? Y **(**Получать адреса DNS-серверов автоматически (Да/Нет)? Да)

    Система устанавливает следующую конфигурацию:
    DHCP включен: Да
    Адреса DNS-серверов: Автоматически

12. Подключите датчик AirMagnet SmartEdge к корпоративной сети с помощью прямого кабеля Ethernet RJ-45.
13. Когда будет предложено перезагрузить датчик, выберите «Да» (Y). После перезагрузки датчика продолжите настройку.
14. Введите: config> show sensor.
    Эта команда выводит список конфигурации.
15. Введите: config > show network.
    Эта команда выводит конфигурацию сети.
16. Введите: config > logout.

Датчик доступен для использования в качестве удаленного устройства поиска и устранения неисправностей.

Веб-страница датчика

Информацию о конфигурации датчика можно просмотреть и изменить, открыв его веб-страницу.

Примечание: В браузере должен быть включен протокол SSL 3.0. Перед подключением к веб-странице датчика отключите брандмауэр компьютера или разрешите порт TCP 443 и кадры UDP в конфигурации брандмауэра.

1. Откройте браузер и введите IP-адрес датчика: например, https://[IP-адрес].
   User Name (Имя пользователя): AirMagnetSensor
   Password (Пароль): Совместно используемый секретный ключ

2. Чтобы изучить доступные страницы датчиков, используйте дерево навигации меню слева.

General Information (Общая информация): Опции меню в этой категории позволяют получить информацию о состоянии датчика и доступ к его журналу.
Diagnostic Information (Диагностическая информация): Опции меню в этой категории предоставляют диагностические тесты и соответствующую информацию для поиска и устранения неисправностей датчика, если в его работе наблюдаются сбои. Если вы считаете, что датчик неисправен, обратитесь в службу технической поддержки. Описание диагностики приводится у правого края страницы диагностики.
Configuration (Конфигурация): Опции меню в этой категории позволяют получить доступ к параметрам конфигурации датчика.

Настройка датчика

Параметр	Описание
Sensor Name (Имя датчика)	Имя датчика по умолчанию «amsensor» можно изменить на уникальное имя, отражающее его физическое местоположение.
Sensor Shared Secret Key (Общий секретный ключ датчика)	Позволяет изменить совместно используемый секретный ключ датчика.
Log Level (Уровень журнала)	В разворачивающемся меню представлены параметры просмотра журнала.
Time Zone (Часовой пояс)	В разворачивающемся меню представлены параметры настройки часового пояса. Выберите регион, соответствующий местоположению датчика AirMagnet SmartEdge.

Network Setup (Настройка сети): Выберите конфигурацию DHCP или Static IP (Статический IP-адрес).

Параметр	Описание
IP Configuration Method (Метод настройки IP)	В разворачивающемся списке выберите Static (Статический) или DHCP. Примечание: Если выбрано Static (Статический), укажите IP-адрес, маску подсети и адрес шлюза. Если же выбрано DHCP, система получит IP-адрес, маску подсети и адрес шлюза автоматически.
IP Address (IP-адрес)	Вводите IP-адрес, ТОЛЬКО если в качестве метода настройки IP выбрано Static (Статический). Смотрите выше.
Subnet Mask (Маска подсети)	Вводите маску подсети, ТОЛЬКО если в качестве метода настройки IP выбрано Static (Статический). Смотрите выше.
Default Gateway (Шлюз по умолчанию)	Вводите IP-адрес шлюза, ТОЛЬКО если в качестве метода настройки IP выбрано Static (Статический). Смотрите выше.
Domain Name (Доменное имя)	Введите доменное имя вашей корпоративной сети, например, mydomain.com
DNS Server Address (Адрес DNS-сервера)	Вводите адрес DNS-сервера, ТОЛЬКО если НЕ отмечено поле Obtain DNS server address automatically (Получать адрес DNS-сервера автоматически).
Alternate DNS Address (Альтернативный адрес DNS)	Вводите альтернативный адрес DNS-сервера, ТОЛЬКО если НЕ отмечено поле Obtain DNS server address automatically (Получать адрес DNS-сервера автоматически).
Alternate DNS Address (2) (Альтернативный адрес DNS (2))	Введите адрес вторичного альтернативного DNS-сервера (при необходимости).
Telnet and SSH Server Options (Параметры сервера Telnet и SSH)	Выберите включение (Enable), если выбрано подключение к датчику с помощью Telnet или SSH.

Factory Default (Заводские настройки по умолчанию): Эта команда позволяет восстановить заводские настройки датчика по умолчанию. Для датчика должно быть установлено «Enterprise Enable» с использованием конфигурации последовательной консоли, как описано в разделе «Настройка конфигурации датчика AirMagnet SmartEdge».
Restart Sensor (Перезапустить датчик): Используйте эту опцию для перезагрузки датчика.
Logout (Выйти): Выход из веб-страницы датчика.

Для подключения к датчику AirMagnet SmartEdge:

Примечание: Перед подключением к датчику выключите брандмауэр компьютера или разрешите TCP-порт 443 и кадры UDP в конфигурации брандмауэра. Кроме того, во время удаленного подключения WFA может обновить датчик до текущего изображения и перезагрузить. Если это произойдет, откроется диалоговое окно, показывающее процесс обновления датчика. Процесс обновления и перезагрузки датчика может занять около 2 минут.

1. Запустите приложение AirMagnet WiFi Analyzer Pro.
2. В меню File (Файл) выберите Connect to (Подключиться к).
3. Выберите AirMagnet Sensor (Датчик AirMagnet).
   - Sensor Name/IP (Имя/IP-адрес датчика): IP-адрес датчика AirMagnet.
   - User Name (Имя пользователя): AirMagnetSensor
   - Password (Пароль): Общий секретный ключ

Примечание: При подключении к датчику конфигурация WiFi Analyzer будет использоваться удаленным датчиком.

Для отключения от датчика AirMagnet SmartEdge:

В меню File (Файл) выберите Disconnect (Отключиться).
В приведенной ниже таблице перечислены функции, недоступные при подключении к удаленному датчику:

Функция	Описание
Wi-Fi Tools (Инструменты Wi-Fi)	Отключены все инструменты, кроме инструментов диагностики (Diagnostic Tools) и инструментов 802.11n (802.11n Tools).
File > Configure (Файл > Настроить)	Вкладка Scan (Сканирование): Скрыта опция Country Code Channel (Канал по коду страны). Вкладка 802.11 отключена. Вкладка Profile (Профиль) отключена.
Live capture (Захват в реальном времени)	Захват на диск отключен.
Roaming Analysis (Анализ роуминга)	Отключено
Compliance Reports (Отчеты о соответствии)	Отключено

Кнопка сброса датчика

Внимание: На датчике AirMagnet SmartEdge имеется кнопка ручного сброса. Прежде чем использовать эту кнопку для сброса настроек датчика, обратитесь в службу технической поддержки для получения инструкций.

Управление сетевыми политиками

О сетевых политиках

В этом разделе объясняется, как настраивать политики безопасности и функционирования беспроводной сети и управлять ими. Из приведенной в предыдущих главах информации очевидно, что сетевая политика является важным компонентом решения AirMagnet. Следовательно, возможность создавать политики и управлять ими для удовлетворения конкретных потребностей своей сети имеет важное значение для успешного внедрения технологии AirMagnet.

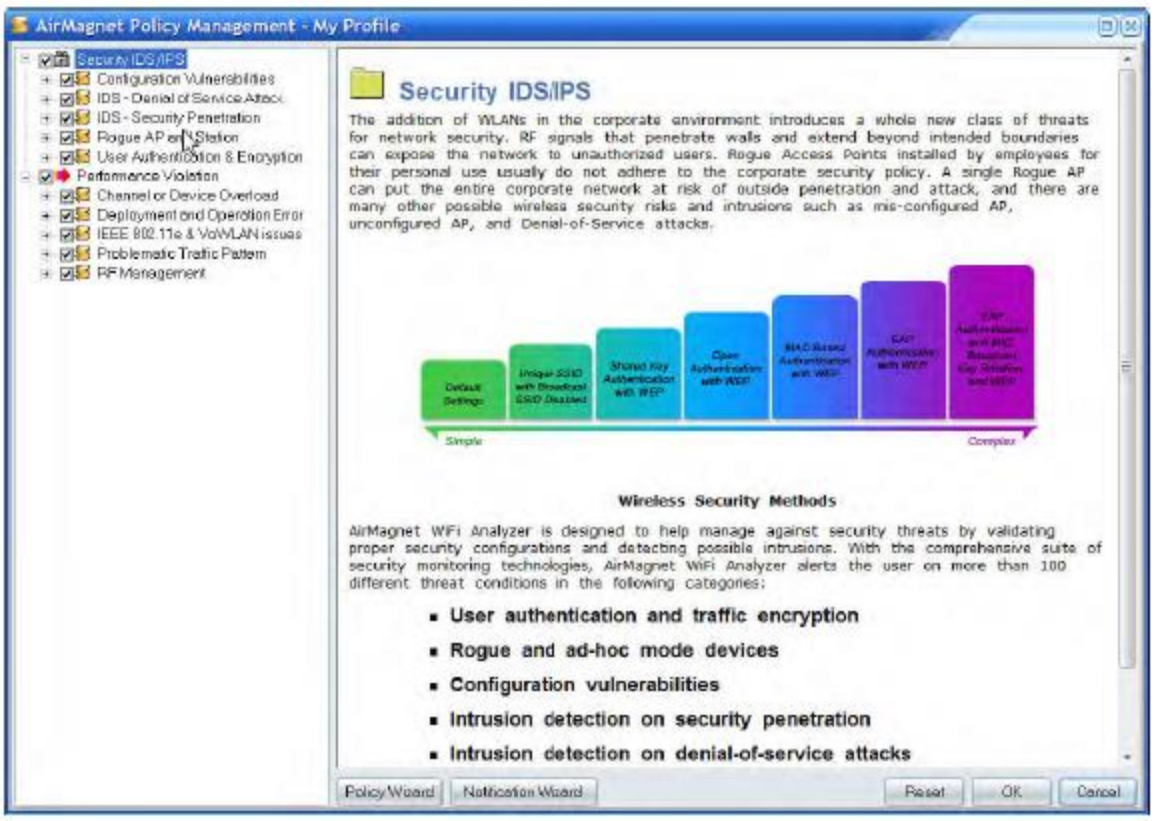
Генерирование аварийных сигналов безопасности и производительности экспертным инструментом AirMagnet AirWISE доказало свою эффективность в управлении сетями WLAN, особенно при управлении крупномасштабными корпоративными сетями WLAN. AirMagnet использует трехуровневую структуру политик, которая значительно упрощает управление и анализ событий на сети WLAN. Понимание этой структурированной конфигурации политики не только помогает администраторам WLAN характеризовать и интерпретировать природу различных нарушений сетевой политики, но также позволяет им при необходимости принимать правильные меры.

Экран Policy Management (Управление политиками)

Управление сетевыми политиками включает в себя создание новых правил политики и изменение или удаление существующих. Все эти задачи выполняются через экран AirMagnet Policy Management (Управление политиками AirMagnet).

Для получения доступа к экрану управления политиками AirMagnet:

1. Щелкните кнопкой мыши на стрелке разворачивающегося списка рядом с иконкой  (Настроить), и выберите Policy Management (Управление политиками). Откроется экран AirMagnet Policy Management.



Как показано на рисунке выше, экран управления политиками AirMagnet состоит из двух частей: дерева политик слева и описания политики справа. Внизу экрана также есть несколько кнопок, предназначенных для управления политиками.

Дерево политик

В дереве политик отображаются все сетевые политики, поддерживаемые AirMagnet. Политики делятся на две основные категории: Security IDS/IPS (система безопасности IDS/IPS (обнаружение/предотвращение проникновения)) и Performance Violation (Нарушение функционирования). Каждую категорию можно разделить еще на несколько подкатегорий. На самом нижнем уровне каждой подкатегории находятся отдельные сигналы тревоги о нарушении политики. Подобная многоуровневая структура упрощает управление сетевыми политиками. Можно щелкнуть кнопкой мыши на значке «плюс», чтобы развернуть узел, или на значке «минус», чтобы его свернуть. Метка в поле означает, что политика активирована. Когда активируется (отмечается) политика верхнего уровня, также активируются все записи под ней. Чтобы отключить тревогу, уберите метку из соответствующего поля.

Описание политики

В разделе описания политики предоставляется подробное объяснение политики или сигнала тревоги, выбранного в дереве политик, а также даются рекомендации по устранению выявленной проблемы. Содержание описания политики напрямую связано с тем, что выбрано в дереве политик.

Управление профилями сетевой политики

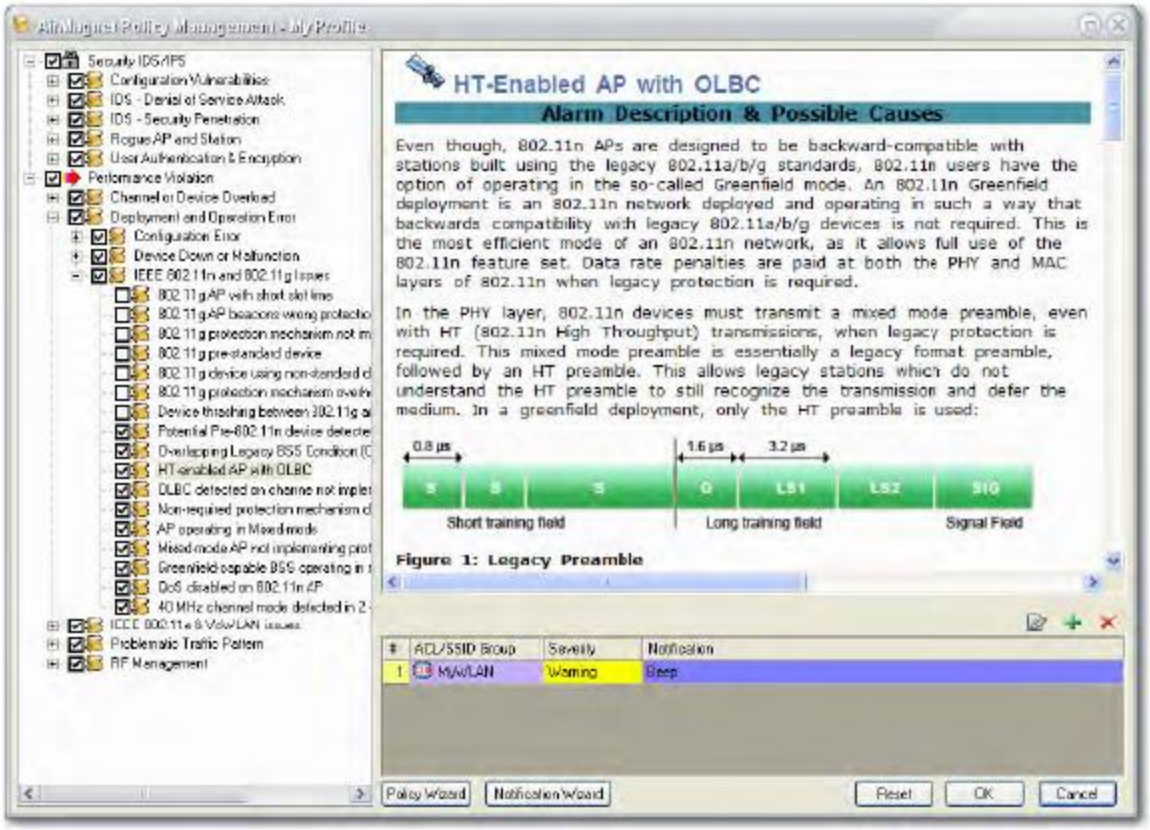
Профиль сетевой политики содержит различные правила политики, которые определяют выдачу сигналов тревоги при нарушении правил, а также способ уведомления ответственных сторон о возникновении сигнала тревоги. Следовательно, управление профилем сетевой политики включает добавление, изменение и/или удаление правил политики, содержащих сигналы тревоги, уведомления и ряд других параметров.

Создание новых правил политики

Правило политики - это набор параметров, выбираемых пользователем в отношении сигнала тревоги. Параметры используются для запуска тревоги, при их нарушении программа генерирует тревогу автоматически. Правила политики являются частью профиля. Профиль приложения AirMagnet WiFi Analyzer по умолчанию уже имеет некоторые предварительно настроенные правила политики, которые отвечают потребностям WLAN в целом. Такие политики по умолчанию будут полезны и обеспечат некоторую базовую защиту беспроводной сети для начинающих пользователей, незнакомых с процедурами управления политиками приложения AirMagnet WiFi Analyzer. Однако, чтобы в полной мере воспользоваться функцией управления политиками приложения AirMagnet WiFi Analyzer, сетевые администраторы должны иметь возможность настраивать и управлять правилами сетевой политики так, чтобы они наилучшим образом соответствовали конкретным потребностям их сетей. В этом разделе объясняются процедуры, связанные с созданием правила политики.

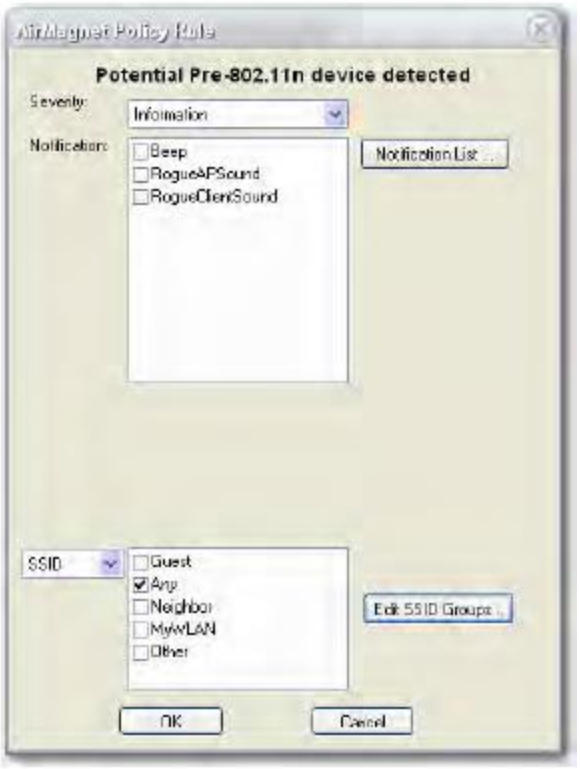
Для создания нового правила политики:

1. На экране управления политиками AirMagnet (AirMagnet Policy Management) разверните дерево политик и выберите нужный сигнал тревоги. Экран управления политиками AirMagnet обновится.



Примечание: Когда в дереве политик выбран сигнал тревоги, в правом нижнем углу экрана управления политиками AirMagnet появляется таблица. В таблице перечислены все правила политики, которые были настроены в отношении этого сигнала тревоги. В то время как многие сигналы тревоги могут иметь несколько правил политики, другие тревоги могут поддерживать только одно правило политики. По умолчанию с сигналом тревоги должно быть связано хотя бы одно правило политики.

2. Щелкните кнопкой мыши на  (Добавить новое правило политики) в правом нижнем углу над таблицей. Откроется диалоговое окно AirMagnet Policy Rule (Правило политики AirMagnet).



3. В диалоговом окне AirMagnet Policy Rule (Правило политики AirMagnet) сделайте необходимые записи и/или выбор.
4. По завершении нажмите кнопку OK.

Запись	Описание
Severity (Серьезность)	Щелкните кнопкой мыши на направленной вниз стрелке и выберите уровень серьезности сигнала тревоги.
Notification (Уведомление)	Укажите метод (методы) уведомления о тревоге, поставив метки в соответствующих полях.
	Примечание: Если необходимо добавить к сигналу тревоги дополнительные опции уведомления, щелкните кнопкой мыши на Notification List… (Список уведомлений). Откроется диалоговое окно AirMagnet Policy Notification List (Список уведомлений для политики AirMagnet), в котором можно настроить дополнительные варианты уведомлений и добавить их в список доступных уведомлений. Для получения подробной информации о том, как настраивать и добавлять параметры уведомлений, обратитесь к разделу «Назначение уведомлений для сигналов тревоги политик».
ACL/SSID	Щелкните кнопкой мыши на направленной вниз стрелке и выберите ACL (список контроля доступа) или идентификатор SSID. Примечание: • Если для использования выбран список контроля доступа (ACL), убедитесь, что он уже настроен. • Если решено использовать SSID, выберите идентификатор SSID из списка справа. • Также можете редактировать идентификаторы SSID, нажав кнопку Edit SSID Groups... (Редактировать группы SSID). Инструкции по редактированию группы SSID приводятся в соответствующем разделе ниже в этой главе.

Изменение существующих правил политики

Приложение AirMagnet WiFi Analyzer поставляется с предварительно настроенными сетевыми политиками и сигналами тревоги. Они предназначены для решения общих проблем безопасности и функционирования беспроводной локальной сети и могут не совсем соответствовать вашей конкретной сети. Кроме того, по мере развития сети любое настроенное правило политики может устареть. Следовательно, профили политик необходимо обновлять, время от времени редактируя правила политики.

Для изменения существующего правила политики:

1. В таблице на экране AirMagnet Policy Management (Управление политикой AirMagnet) выберите нужное правило политики и щелкните кнопкой мыши на  (Изменить правило политики). Откроется диалоговое окно AirMagnet Policy Rule (Правило политики AirMagnet).
2. Внесите в диалоговом окне правила политики AirMagnet желаемые изменения.
3. По завершении нажмите кнопку OK.

Удаление существующих правил политики

По мере развития беспроводной локальной сети некоторые правила в профиле политики могут устареть настолько, что их следует удалить из профиля. Важно отметить, что приложение AirMagnet WiFi Analyzer требует, чтобы с тревогой было связано хотя бы одно правило политики. По этой причине правило политики невозможно будет удалить, если оно является единственным в таблице политик.

Для удаления правила политики:

1. На экране AirMagnet Policy Management (Управление политикой AirMagnet) выделите нужное правило политики.
2. Щелкните кнопкой мыши на  (Удалить правило политики).
3. Появится окно подтверждения. Нажмите Yes (Да).

Назначение уведомлений политикам

Уведомления являются важной частью правил политики. Это способы, которые приложение AirMagnet WiFi Analyzer использует для уведомления ответственных сторон о появлении сигналов тревоги для политик. Приложение AirMagnet WiFi Analyzer предоставляет несколько вариантов уведомлений. Управление уведомлениями о сигналах тревоги включает в себя настройку вариантов уведомления и их назначение для сигналов тревоги.

Добавление вариантов уведомления к тревоге

Каждый сигнал тревоги может быть связан с одним или несколькими вариантами уведомления. Это позволит уведомлять ответственные стороны всякий раз, когда сигнал тревоги появляется. Невыполнение данного требования может привести к задержке реакции на надвигающиеся угрозы, что поставит под угрозу безопасность и функционирование всей вашей сети. Добавление вариантов уведомлений включает в себя назначение большего количества вариантов уведомления сигналу тревоги при условии, что эти параметры применимы к сигналу тревоги. Также может потребоваться настроить некоторые новые опции с нуля, а затем назначить их сигналу тревоги.

Для добавления уведомления к тревоге:

1. В дереве политик на экране AirMagnet Policy Management (Управление политикой AirMagnet) выделите нужный сигнал тревоги. Экран управления политиками AirMagnet обновится, и на нем будет показана таблица правил политики, содержащая все правила политики для данного сигнала тревоги.
2. В таблице правил политики выделите правило (или определенное правило политики, если существует более одного правила политики) и щелкните кнопкой мыши на  (Изменить правило политики). Откроется диалоговое окно AirMagnet Policy Rule (Правило политики AirMagnet).

Примечание: По умолчанию приложение AirMagnet WiFi Analyzer поставляется с тремя доступными для использования базовыми опциями уведомлений, а звуковой сигнал (Beep) назначается всем сигналам тревоги в любом предварительно настроенном профиле/правиле политики. Однако вы можете настроить другие расширенные опции уведомлений, которые поддерживает приложение AirMagnet WiFi

Analyzer, и добавить их в список доступных уведомлений в диалоговом окне AirMagnet Policy Rule (Правило политики AirMagnet), где их можно будет назначить выбранному сигналу тревоги. В следующих шагах данной процедуры показано, как настроить и назначить опции уведомления сигналу тревоги.

3. Если необходимо назначить сигналу тревоги любой из доступных и применимых вариантов уведомления, поставьте метки в соответствующих полях и нажмите кнопку OK.

Примечание: После нажатия кнопки OK диалоговое окно AirMagnet Policy Rule (Правило политики AirMagnet) закрывается, а выбранные опции уведомления добавляются в поле Notification (Уведомление) таблицы политик на экране AirMagnet Policy Management (Управление политикой AirMagnet).

4. Если необходимо настроить и использовать некоторые другие опции уведомления, нажмите кнопку Notification List… (Список уведомлений). Появится список уведомлений политики AirMagnet (AirMagnet Policy Notification List).

Примечание: В диалоговом окне AirMagnet Policy Notification List (Список уведомлений политики AirMagnet) можно создавать и/или изменять варианты уведомления, которые затем можно отправить в список доступных вариантов уведомления в диалоговом окне AirMagnet Policy Rule (Правило политики AirMagnet). Поэтому он содержит те же варианты, что и диалоговое окно правила политики AirMagnet.

5. Щелкните кнопкой мыши на  (Добавить новое уведомление). Откроется диалоговое окно Notification Type Select (Выбор типа уведомления).

Примечание: Диалоговое окно Notification Type Select (Выбор типа уведомления) содержит расширенные варианты уведомлений, которые поддерживает приложение AirMagnet WiFi Analyzer. Эти варианты требуют индивидуальной настройки в каждом конкретном случае. Обзора всех вариантов приводится в таблице ниже.

Вариант	Описание
Email (Электронная почта)	Позволяет настроить передачу уведомления о тревоге по электронной почте. Для использования этого варианта необходимо настроить основные параметры электронной почты (имя и пароль учетной записи, сервер исходящей почты и т.д.).
SMS Via Email (SMS по электронной почте)	Данный вариант похож на базовый вариант использования электронной почты, за исключением того, что отправляется текстовое сообщение, которое можно получить на мобильный телефон. Потребуется ввести номер своего пейджера/телефона и SMS-сервер.
Page over Phone (Поисковый вызов через телефон)	Можно настроить передачу поискового вызова на пейджер/телефон при появлении сигнала тревоги. Нужно будет ввести номер TAP-сервера, с которого будут отправляться поисковые вызовы.
Page over Internet (Поисковый вызов через Интернет)	Этот вариант аналогичен выбору Page over Phone (Поисковый вызов через телефон), но для отправки поискового вызова используется служба Интернет-пейджинга. Вместо номера сервера TAP нужно будет ввести сервер SNPP.
Play Sound (Воспроизвести звук)	Базовый вариант уведомления, позволяющий просто назначить звуковой файл для предупреждения пользователя о появлении сигнала тревоги.
SysLog (Системный журнал)	Данный вариант позволяет записать предупреждение о тревоге в системный журнал Windows. Потребуется направить его на свой сервер SysLog.

6. Выберите подходящий вариант в диалоговом окне Notification Type Select (Выбор типа уведомления) и нажмите кнопку OK. Появится уникальное диалоговое окно, в котором можно будет настроить вариант уведомления.
7. Настройте вариант и нажмите кнопку OK. Диалоговое окно для выбранной конфигурации уведомлений будет закрыто.
8. Чтобы закрыть диалоговое окно AirMagnet Policy Notification List (Список уведомлений политики AirMagnet), нажмите кнопку OK.
9. В диалоговом окне AirMagnet Policy Rule (Правило политики AirMagnet) выберите вновь созданный вариант уведомления и нажмите кнопку OK. Вариант уведомления будет добавлен в таблицу политик на экране управления политиками AirMagnet.
10. Чтобы закрыть экран управления политиками AirMagnet, нажмите кнопку OK.

Изменение вариантов уведомления о тревоге

Изменение уведомлений о сигналах тревоги включает изменение вариантов передачи уведомления, назначенных для сигнала тревоги. Существующий вариант уведомления можно заменить другим вариантом при условии, что новый вариант применим к сигналу тревоги или можно изменить конфигурацию существующего варианта уведомления.

Для изменения существующего уведомления о тревоге:

1. В таблице правил политики на экране управления политикой AirMagnet (AirMagnet Policy Management) выделите правило политики и щелкните кнопкой мыши на Edit Policy Rule (Изменить правило политики). Откроется диалоговое окно AirMagnet Policy Rule (Правило политики AirMagnet).
2. Если необходимо заменить существующий вариант уведомления другим доступным вариантом, снимите метку из поля существующего варианта и поставьте в поле другого варианта из списка доступных, затем нажмите кнопку OK.

Примечание: После нажатия кнопки OK диалоговое окно AirMagnet Policy Rule (Правило политики AirMagnet) закроется, и в таблице политик на экране AirMagnet Policy Management (Управление политикой AirMagnet) появится новый назначенный вариант уведомления, заменивший предыдущий старый вариант уведомления.

3. Если необходимо изменить настройки существующего варианта уведомления, нажмите кнопку Notification List… (Список уведомлений). Появится список уведомлений политики AirMagnet (AirMagnet Policy Notification List).

4. Выделите вариант уведомления и щелкните кнопкой мыши на  (Изменить уведомление). Появится диалоговое окно конфигурации для варианта уведомления.

Примечание: Поскольку изменяются настройки существующего варианта уведомления, имя уведомления отображается серым цветом. Это означает, что имя уведомления изменить невозможно.

5. Внесите необходимые изменения в диалоговом окне конфигурации и нажмите кнопку OK, чтобы закрыть это диалоговое окно. Внесенные изменения появятся в диалоговом окне AirMagnet Policy Notification List (Список уведомлений политики AirMagnet).
6. Нажмите кнопку OK, чтобы закрыть диалоговое окно AirMagnet Policy Notification List (Список уведомлений политики AirMagnet).
7. Нажмите кнопку OK, чтобы закрыть диалоговое окно AirMagnet Policy Rule (Правило политики AirMagnet).
8. Нажмите кнопку OK, чтобы закрыть экран управления политиками AirMagnet (AirMagnet Policy Management). Внесенные в вариант уведомления изменения будут реализованы в правиле политики для выбранного сигнала тревоги.

Удаление существующих уведомлений о тревоге

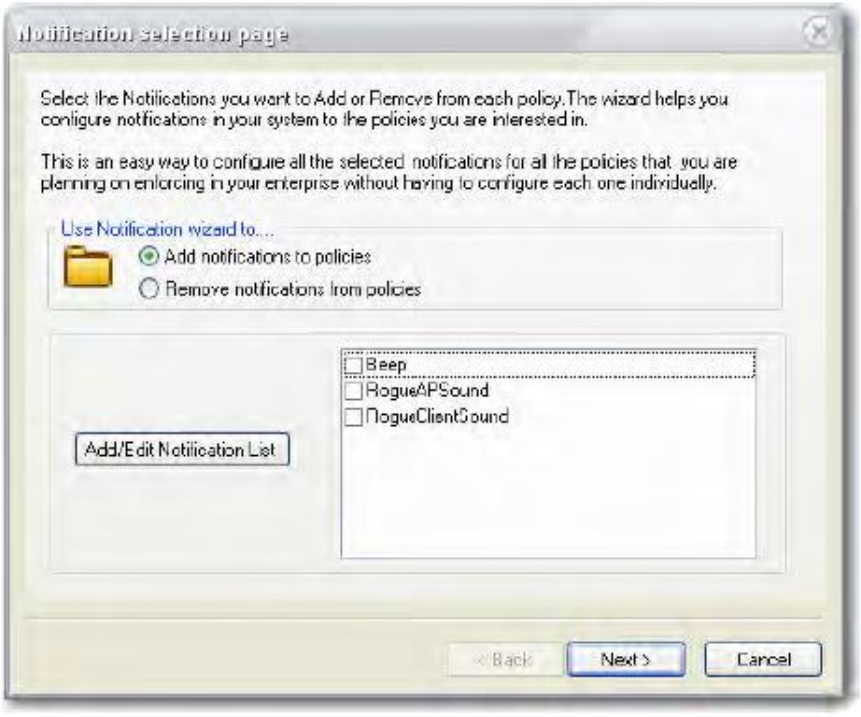
Диалоговое окно AirMagnet Policy Rule содержит все настроенные варианты уведомлений. Хотя можно назначить или удалить любой из них для сигнала тревоги из диалогового окна правила политики AirMagnet (AirMagnet Policy Rule), если вы хотите удалить его навсегда из профиля политики, то должны удалить из диалогового окна AirMagnet Policy Notification List (Список уведомлений политики AirMagnet).

Для удаления варианта уведомления о тревоге:

1. В диалоговом окне AirMagnet Policy Notification List (Список уведомлений политики AirMagnet) выделите вариант уведомления, который необходимо удалить, и щелкните кнопкой мыши на  (Удалить уведомление). Появится окно подтверждения.
2. Для подтверждения нажмите Yes (Да). Выбранный вариант уведомления исчезнет из диалогового окна AirMagnet Policy Notification List.
3. Нажмите кнопку OK, чтобы закрыть диалоговое окно AirMagnet Policy Notification List (Список уведомлений политики AirMagnet).
4. Нажмите кнопку OK, чтобы закрыть диалоговое окно AirMagnet Policy Rule (Правило политики AirMagnet).
5. Нажмите кнопку OK, чтобы закрыть экран управления политиками AirMagnet (AirMagnet Policy Management).

Примечание: Вариант уведомления будет навсегда удален из текущего профиля политики. Если необходимо удалить один и тот же вариант уведомления из всех других профилей политики, нужно удалять его из всех профилей по очереди. Для восстановления удаленного варианта уведомления потребуется переустановить приложение WiFi Analyzer.

Назначение уведомлений для сигналов тревоги политики



Для назначения уведомления политикам или сигналам тревоги:

1. На экране AirMagnet Policy Management (Управление политиками AirMagnet) нажмите кнопку Notification Wizard (Мастер уведомлений). Появится страница выбора уведомлений (Notification Selection Page).
2. Выберите опцию Add Notifications to Policy (Добавить уведомления в политику).
3. Выберите уведомление (или уведомления) и нажмите кнопку Next (Далее). Откроется страница выбора политики (Policy Selection Page).

4. Выберите политики и тревоги, к которым необходимо применить уведомления.
5. Выберите уровень серьезности, при котором должно создаваться уведомление, и нажмите кнопку Next (Далее). Появится страница подтверждения.
6. Нажмите Finish (Готово). Выбранные уведомления будут назначены политикам и сигналам тревоги.

По умолчанию каждый сигнал тревоги содержит только одно уведомление. Для большинства сигналов тревоги уведомление по умолчанию – это короткий звуковой сигнал, но для неавторизованных точек доступа и клиентов уведомлением по умолчанию является звуковое предупреждение. При необходимости можно добавлять, изменять или удалять уведомления.

Назначение политик группам ACL или SSID

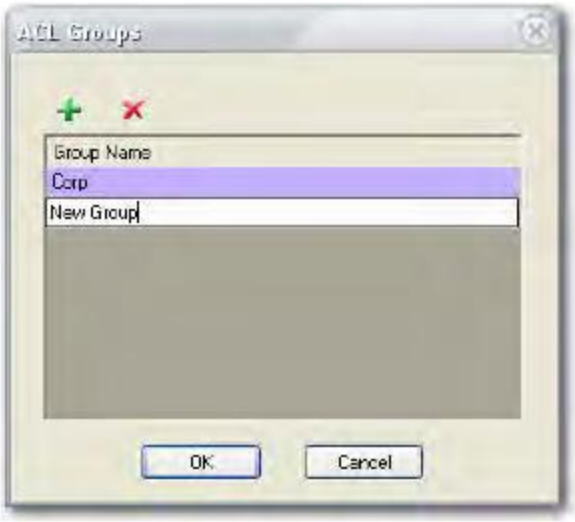
Как упоминалось ранее, группы ACL и SSID также являются важной частью профилей сетевой политики AirMagnet и играют жизненно важную роль в управлении сетевой безопасностью и функционированием. Каждая группа ACL или SSID содержит информацию о конкретных беспроводных устройствах. Когда политики назначаются группам ACL или SSID в правиле политики, оно сообщает программе, что только те устройства, которые принадлежат к группам ACL или SSID, являются допустимыми, и что любое устройство за пределами указанных групп ACL или SSID будет рассматриваться как мошенническое, и при обнаружении вызовет подачу сигнала тревоги.

Использование ACL или SSID в правиле политики зависит от выбранного сигнала тревоги. Хотя некоторые сигналы тревоги могут быть связаны только с ACL, другие могут применяться только к SSID. Также существуют сигналы тревоги, которые могут применяться либо к ACL, либо к SSID. Таким образом, при настройке правил политики, связанных с различными сигналами тревоги, в диалоговом окне AirMagnet Policy Rule можно будет заметить определенные различия.

Назначение политик группам ACL

Группа ACL (Список контроля доступа) – это список беспроводных устройств, сгруппированных по MAC-адресу. Приложение AirMagnet WiFi Analyzer использует группы ACL для эффективного управления и контроля доступа к беспроводной сети. Когда группа ACL назначается политике, она становится источником запуска сигнала тревоги, которому она назначена. Доступ к сети будет предоставлен только устройствам в группе ACL. Любому устройству, не входящему в группу ACL, не только будет отказано в доступе, но всякий раз, когда такое устройство будет обнаружено в сети, будет инициирована тревога.

Для назначения политики группе ACL:



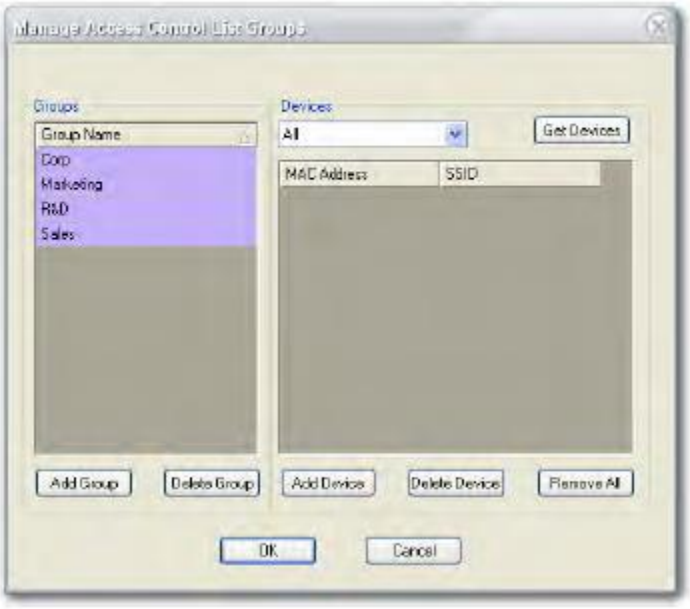
1. В диалоговом окне AirMagnet Policy Rule (Правило политики AirMagnet) щелкните кнопкой мыши на Edit ACL Groups… (Редактировать группы ACL). Появится диалоговое окно ACL Groups (Группы ACL).
2. В диалоговом окне ACL Groups (Группы ACL) щелкните кнопкой мыши на  (Добавить новую группу ACL). В таблице появится новая запись New Group (Новая группа).
3. Выделите запись, введите поверх нее уникальное имя, затем нажмите кнопку OK. Новая группа ACL будет добавлена в список доступных групп ACL в диалоговом окне AirMagnet Policy Rule (Правило политики AirMagnet).
4. Выберите только что созданную группу ACL и нажмите кнопку OK, чтобы закрыть диалоговое окно AirMagnet Policy Rule.
5. Нажмите кнопку OK, чтобы закрыть экран управления политиками AirMagnet (AirMagnet Policy Management).

Примечание: Описанные выше шаги с 1 по 5 позволяют создать новую группу ACL, которая на данный момент пуста, поскольку в нее не были добавлены какие-либо устройства. Чтобы включить группу ACL в управление политиками, необходимо добавить в нее устройства. Ниже показано, как добавить устройства в группу ACL.

Добавление устройств в группу ACL

Для добавления устройств в группу ACL:

1. На странице Start щелкните кнопкой мыши на  . Откроется диалоговое окно AirMagnet Config (Конфигурация AirMagnet).
2. Щелкните кнопкой мыши на Manage ACL Groups… (Управлять группами ACL). Откроется диалоговое окно Manage Access Control List (Управление списком контроля доступа).



Примечание: Corp является группой ACL по умолчанию, которая содержит все устройства, обнаруженные приложением AirMagnet WiFi Analyzer в вашей сети. Необходимо создать новые группы ACL и назначить устройства различным группам. Описание кнопок в диалоговом окне Manage Access Control List (Управление списком контроля доступа) приводится в таблице ниже.

Опция	Описание
Devices (Устройства)	В этом разворачивающемся списке можно указать тип устройств, которые необходимо включить в группу (точка доступа AP, станция STA или устройство Ad-Hoc).
Get Devices (Получить устройства)	Данная кнопка открывает диалоговое окно Filter Devices (Фильтровать устройства) и позволяет сканировать устройства для добавления в выбранную группу.
Add Group (Добавить группу)	Данная кнопка позволяет создать новую группу ACL. Для переименования группы дважды щелкните кнопкой мыши на имени группы и введите собственное имя.
Delete Group (Удалить группу)	Данная кнопка позволяет удалить выбранную группу ACL.
Add Device (Добавить устройство)	Данная кнопка позволяет добавить устройство вручную, введя его MAC-адрес.
Delete Device (Удалить устройство)	Данная кнопка позволяет удалить выбранное устройство.
Remove All (Убрать все)	Данная кнопка позволяет удалить все записи об устройствах в выбранной группе.

3. Выберите имя вновь созданной группы ACL (например, «QA»).
4. Нажмите Remove All (Убрать все), чтобы убрать устройства из таблицы.

5. Щелкните кнопкой мыши на Get Devices (Получить устройства). Откроется диалоговое окно Filter Devices (Фильтровать устройства).

6. Используйте три фильтра для выбора устройств, которые будут добавлены в группу ACL, и нажмите кнопку OK, чтобы закрыть диалоговое окно Filter Devices. Описание опций фильтра приводится в таблице ниже.

Поле	Описание
Vendor ID (Идентификатор производителя)	Это поле позволяет выбрать производителя ваших сетевых устройств. Список будет фильтроваться автоматически для включения только устройств этого конкретного производителя.
SSID	Это поле позволяет добавлять только устройства, использующие определенный идентификатор SSID.
Device Type (Тип устройства)	Это поле позволяет указать тип устройства, которое необходимо добавить (точка доступа AP, станция STA или устройство Ad-Hoc).

7. Нажмите кнопку OK, чтобы закрыть диалоговое окно Manage Access Control List Groups (Управление группами списков контроля доступа).
8. Нажмите кнопку OK, чтобы закрыть диалоговое окно AirMagnet Config. Группа ACL «QA» теперь заполнена указанными вами устройствами.

Назначение политик группам SSID

Группы SSID также можно привязать к сетевым политикам для защиты беспроводной сети от потенциальных угроз безопасности и функционированию. Это делается путем помещения беспроводных устройств в разные группы SSID и последующего назначения им политик. Это еще один эффективный способ применения сетевых политик к устройствам.

Назначение политик существующим группам SSID

Существующая группа SSID – это группа, которая уже находится в диалоговом окне правила политики AirMagnet (AirMagnet Policy Rule), когда это окно открывается. Приложение AirMagnet WiFi Analyzer поставляется со списком групп SSID, которые можно использовать сразу.

Для назначения политики существующей группе SSID:

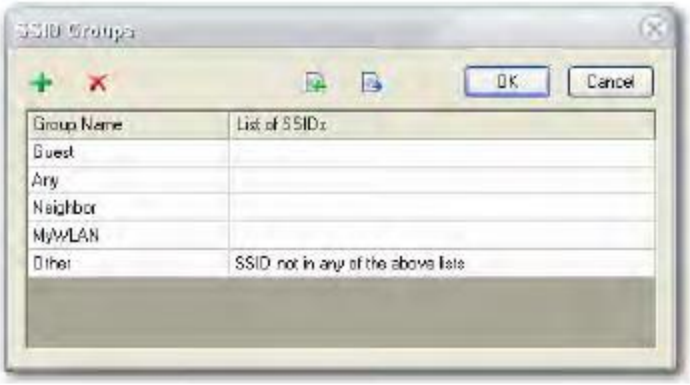
1. На экране AirMagnet Policy Management (Управление политикой AirMagnet) выберите политику и нажмите Add Policy Rule (Добавить правило политики). Откроется диалоговое окно AirMagnet Policy Rule (Правило политики AirMagnet).
2. Выберите группу или группы SSID, поставив метки в соответствующих полях.
3. Нажмите кнопку OK.

Изменение существующих групп SSID

Существующие группы SSID удобны при назначении им политик. Иногда может потребоваться изменить существующую группу SSID перед назначением ей политик. Изменение группы SSID может включать изменение ее имени, а также идентификаторов SSID в ней.

Для изменения существующей группы SSID:

1. В диалоговом окне AirMagnet Policy Rule (Правило политики AirMagnet) нажмите Edit SSID Groups… (Изменить группы SSID). Появится диалоговое окно SSID Groups (Группы SSID).



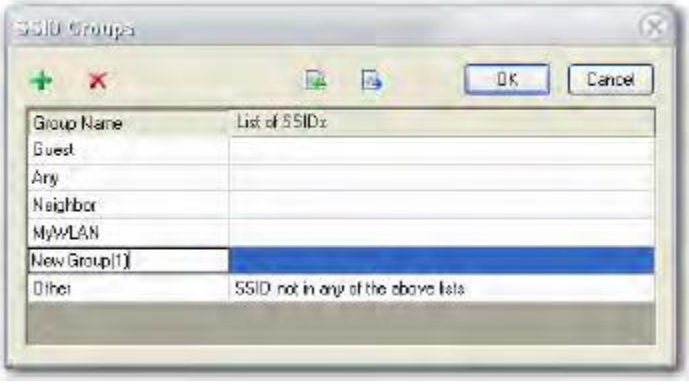
2. Щелкните кнопкой мыши, чтобы выделить имя группы SSID, и введите поверх него уникальное имя (если хотите переименовать группу). Обратите внимание, что предварительно созданные группы переименовать невозможно.
3. Щелкните кнопкой мыши, чтобы выделить соответствующее поле списка SSID (SSID List), и введите идентификаторы SSID, которые будут включены в группу SSID. Записи чувствительны к регистру и должны быть разделены запятыми (пример записи: SSID1, SSID2 и т.д.).
4. Нажмите кнопку OK, чтобы закрыть диалоговое окно SSID Groups (Группы SSID).
5. В диалоговом окне Policy Rule (Правило политики) выберите группу SSID и нажмите кнопку OK.

Создание новой группы SSID

Приложение AirMagnet WiFi Analyzer также позволяет создавать группы SSID с нуля, если это необходимо.

Для создания новой группы SSID:

1. В диалоговом окне SSID Groups (Группы SSID) щелкните кнопкой мыши на  (Новая группа SSID). В диалоговом окне появится новая запись с пометкой New Group (Новая группа).



2. Выделите новую запись и введите поверх нее уникальное имя.

3. Выделите поле SSID List (Список SSID) и введите идентификаторы SSID, которые будут включены в эту группу.
4. Нажмите кнопку OK, чтобы закрыть диалоговое окно SSID Groups (Группы SSID).
5. В диалоговом окне AirMagnet Policy Rule (Правило политики AirMagnet) выберите только что созданную группу SSID.
6. Нажмите кнопку OK, чтобы закрыть диалоговое окно AirMagnet Policy Rule.

Удаление существующей группы SSID

Из-за обновления сети некоторые группы SSID могут со временем устареть. В результате может потребоваться удалить эти устаревшие группы SSID из таблицы SSID Groups (Группы SSID).

Для удаления группы SSID:
1. На экране SSID Groups (Группы SSID) выделите определенный идентификатор SSID.
2. Щелкните кнопкой мыши на  (Удалить выбранную группу SSID).
3. Нажмите кнопку OK.

Удаление существующих уведомлений

Для удаления существующего уведомления:
1. На экране AirMagnet Policy Notification List (Список уведомлений политики AirMagnet) выделите определенную запись.
2. Нажмите Delete Notification (Удалить уведомление). Появится экран подтверждения.
3. Нажмите Yes (Да).

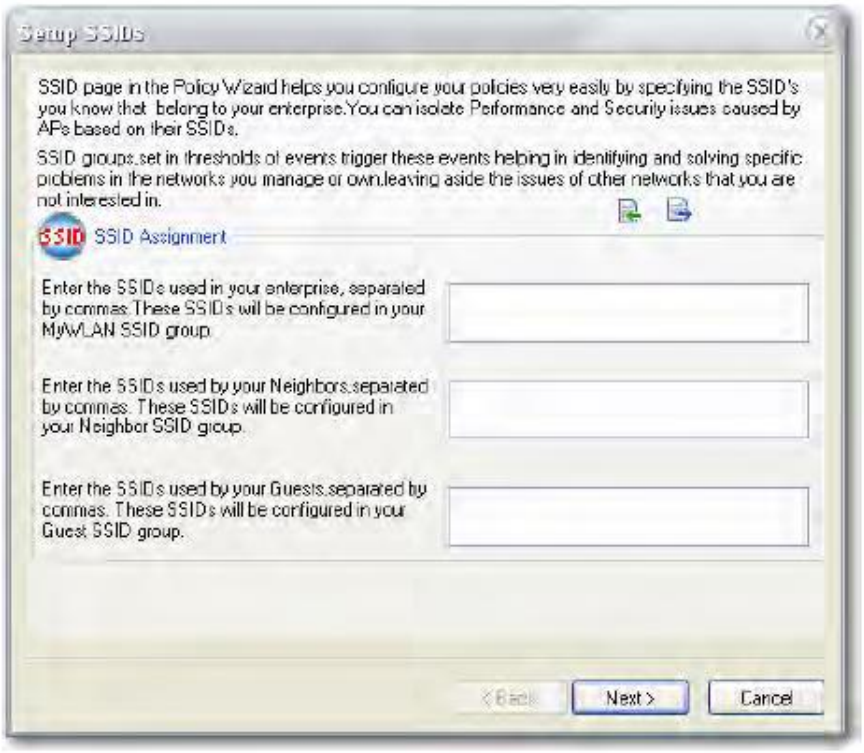
Работа с мастером политик

Мастер политик (Policy Wizard) предоставляет простой способ настройки политики безопасности и функционирования сети WLAN, подходящий даже для начинающих пользователей. Это позволит вам настраивать политики WLAN на основе собственных знаний настроек своей сети. Данная утилита дает начинающим пользователям, не знакомым с механизмами управления политиками приложения AirMagnet WiFi Analyzer. возможность быстрого и легкого запуска.

Настройка политик с помощью мастера политик

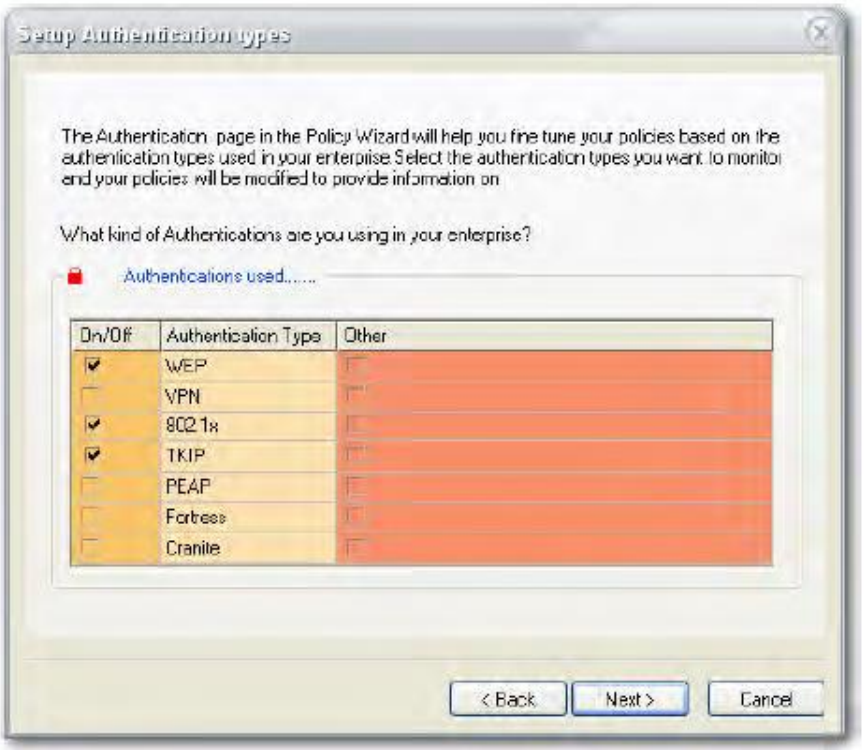
Мастер настройки политик проведет вас через весь процесс настройки, используя всего несколько простых экранов, которые охватывают следующие области:

- Setting up SSID Groups (Настройка групп SSID) – Эта опция запрашивает используемые вашим предприятием, соседними предприятиями и вашими гостями идентификаторы SSID сети WLAN.
- Setting up Authentication (Настройка аутентификации) – Позволяет настраивать политики на основе типов аутентификации, используемых на вашем предприятии, соседних предприятиях и вашими гостями. В этом случае система автоматически уведомит вас о нарушении выбранных типов аутентификации.
- Setting up Vendor Lists (Настройка списков поставщиков) – Данная опция позволяет связать конфигурацию политики с аппаратными устройствами, используемыми на вашей сети. Производители точек доступа и станций указываются в отдельных полях. Таким образом, система сможет подать сигнал тревоги, если в вашей сети будет обнаружено любое аппаратное устройство, отличное от указанного вами.

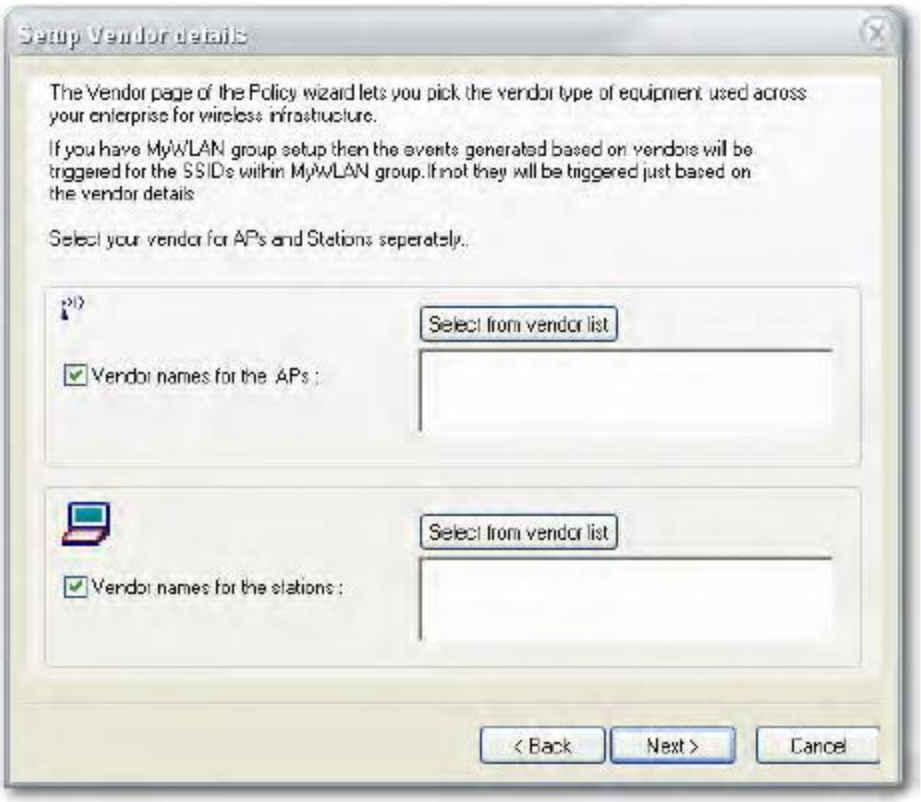


Для настройки политик с помощью мастера Policy Wizard:

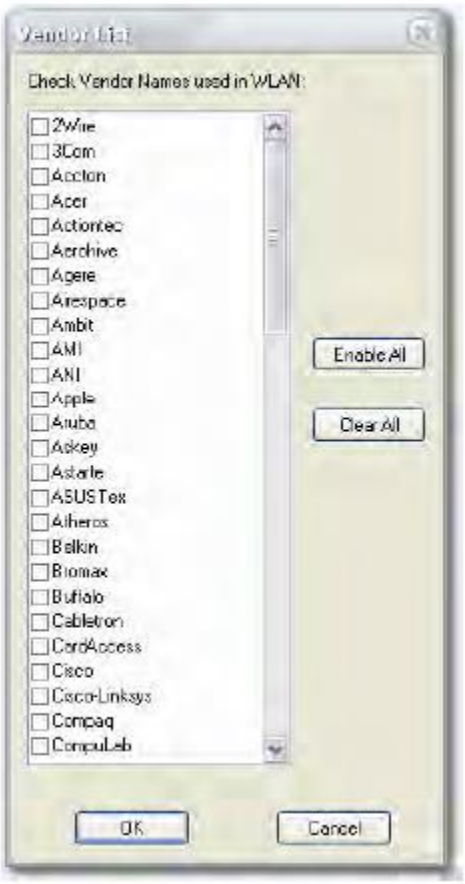
1. На экране AirMagnet Policy Management (Управление политиками AirMagnet) нажмите кнопку Policy Wizard (Мастер политик). Появится экран Setup SSIDs (Настроить SSID).
2. Введите идентификаторы SSID, используемые вашим предприятием, соседями и гостями, и нажмите кнопку Next (Далее). Появится экран Setup Authentication Types (Настройка типов аутентификации).



3. Выберите тип (или типы) аутентификации для своей сети, а также для соседней, гостевой и других сетей. Нажмите кнопку Next (Далее). Появится экран Setup Vendor List (Настроить список производителей).



4. Поставьте метку в поле Vendor Names for the APs (Имена производителей точек доступа) и нажмите кнопку Select from Vendor List (Выбрать из списка производителей). Появится экран Vendor List (Список производителей).



5. Выберите тех производителей, точки доступа которых используются в корпоративной сети, и нажмите кнопку OK. Имена выбранных производителей появятся в разделе AP (Точки доступа).
6. Повторите шаги с 4 по 5 для настройки списка производителей станций (Vendor List of Stations).
7. Затем нажмите кнопку Next (Далее). Появится экран подтверждения.
8. Нажмите кнопку Finish (Готово).

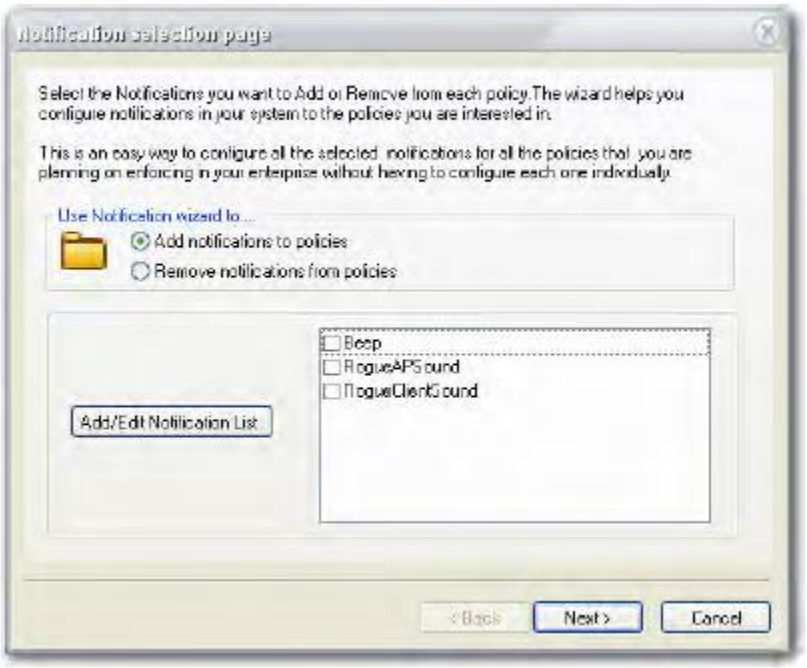
Работа с мастером уведомлений

Уведомления - это способы, которыми приложение AirMagnet WiFi Analyzer уведомляет назначенную сторону о нарушениях политики. Мастер уведомлений (Notification Wizard) разработан для того, чтобы помочь начинающим пользователям легко настраивать уведомления о сигналах тревоги и применять их в сетевых политиках. Используя последовательность экранов, мастер уведомлений сможет быстро провести вас по основным этапам настройки уведомлений, что даст вам возможность быстро перейти к настройке политики.

Назначение уведомлений для сигналов тревоги политики

Для назначения уведомление политикам или сигналам тревоги:

1. На экране AirMagnet Policy Management (Управление политиками AirMagnet) нажмите кнопку Notification Wizard (Мастер уведомлений). Появится страница выбора уведомлений (Notification Selection Page).



2. Выберите опцию Add Notifications to Policies (Добавить уведомления в политики).

3. Выберите уведомление (или уведомления) и нажмите кнопку Next (Далее). Откроется страница выбора политики (Policy Selection Page).

4. Выберите политики и сигналы тревоги, к которым необходимо применить уведомление (уведомления).
5. Выберите уровень серьезности, при котором должно создаваться уведомление, и нажмите кнопку Next (Далее). Появится страница подтверждения.
6. Нажмите кнопку Finish (Готово). Выбранные уведомления будут назначены политикам и сигналам тревоги.

По умолчанию каждый сигнал тревоги содержит только одно уведомление. Для большинства сигналов тревоги уведомлением по умолчанию является короткий звуковой сигнал, но для неавторизованных точек доступа и клиентов уведомлением по умолчанию является звуковое предупреждение. При необходимости можно добавлять, изменять или удалять уведомления.

Другие элементы управления на экране управления политиками

На экране управления политикой AirMagnet (AirMagnet Policy Management) также имеются следующие кнопки управления:

- Reset (Сброс) – Позволяет восстановить исходные параметры политики, установленные производителем.
- OK – Позволяет подтвердить только что созданный или измененный параметр политики.
- Cancel (Отмена) – Позволяет отменить все внесенные пользователем дополнения или изменения и вернуть систему к ранее сохраненным настройкам.

Процедуры управления политикой AirMagnet

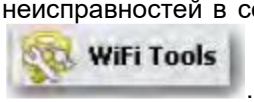
Приведенные ниже шаги призваны проиллюстрировать процесс расширения структуры политики на экране AirMagnet Policy Management:

1. Выберите группу политик, например, Security (Безопасность).
2. Выберите категорию политики в этой группе политик, например, User Authentication and Encryption (Аутентификация пользователя и шифрование).
3. Выберите подкатегорию выбранной категории политики, например, WPA-802.1x & TKIP.
4. Выделите конкретный сигнал тревоги в подкатегории политики, например, 802.1x Rekey Timeout Too Long (Слишком большой интервал смены ключей 802.1x).

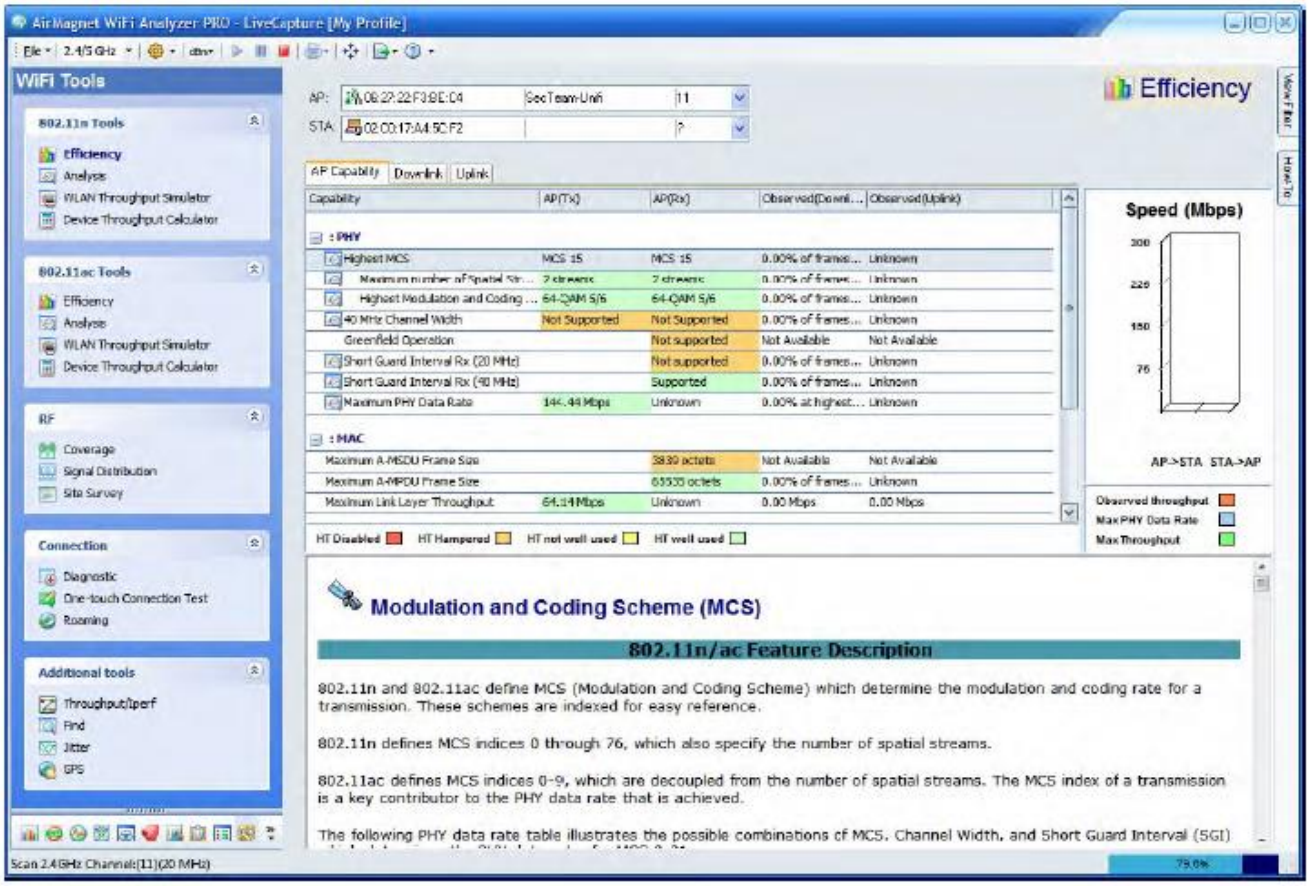
Подробное описание политик AirMagnet в сети WLAN приводится в «Справочном руководстве по политикам AirMagnet в беспроводной локальной сети», которое находится на компакт-диске с программным обеспечением.

Экран WiFi Tools (Инструменты WiFi)

Об экране WiFi Tools (Инструменты WiFi)

Экран WiFi Tools (Инструменты WiFi) содержит инструменты, предназначенные для поиска и устранения неисправностей в сети 802.11. Чтобы перейти к экрану инструментов WiFi, щелкните кнопкой мыши на 

. На приведенном ниже рисунке показан экран инструментов WiFi.



Как показано на экране, приложение AirMagnet WiFi Analyzer предоставляет пользователю следующие инструменты:

- Измерение эффективности сети 802.11n и 802.11ac
- Анализ сетевых проблем 802.11n и 802.11ac
- Моделирование пропускной способности WLAN для 802.11n и 802.11ac
- Расчет пропускной способности устройства для 802.11n и 802.11ac
- Измерение покрытия сети WLAN или отдельной соты (ячейки) сети
- Распределение радиочастотного сигнала на объекте
- Проведение обследования объекта
- Выполнение диагностики сети WLAN
- Отслеживание сетевого устройства
- Проведение тестов роуминга
- Измерение производительности сети WLAN с помощью Iperf
- Измерение джиттера радиочастотного сигнала
- Поиск устройств в сети WLAN
- Измерение производительности выгрузки и загрузки для FTP
- Измерение производительности выгрузки и загрузки для HTTP
- Тестирование веб-доступа

Инструменты 802.11n/ac

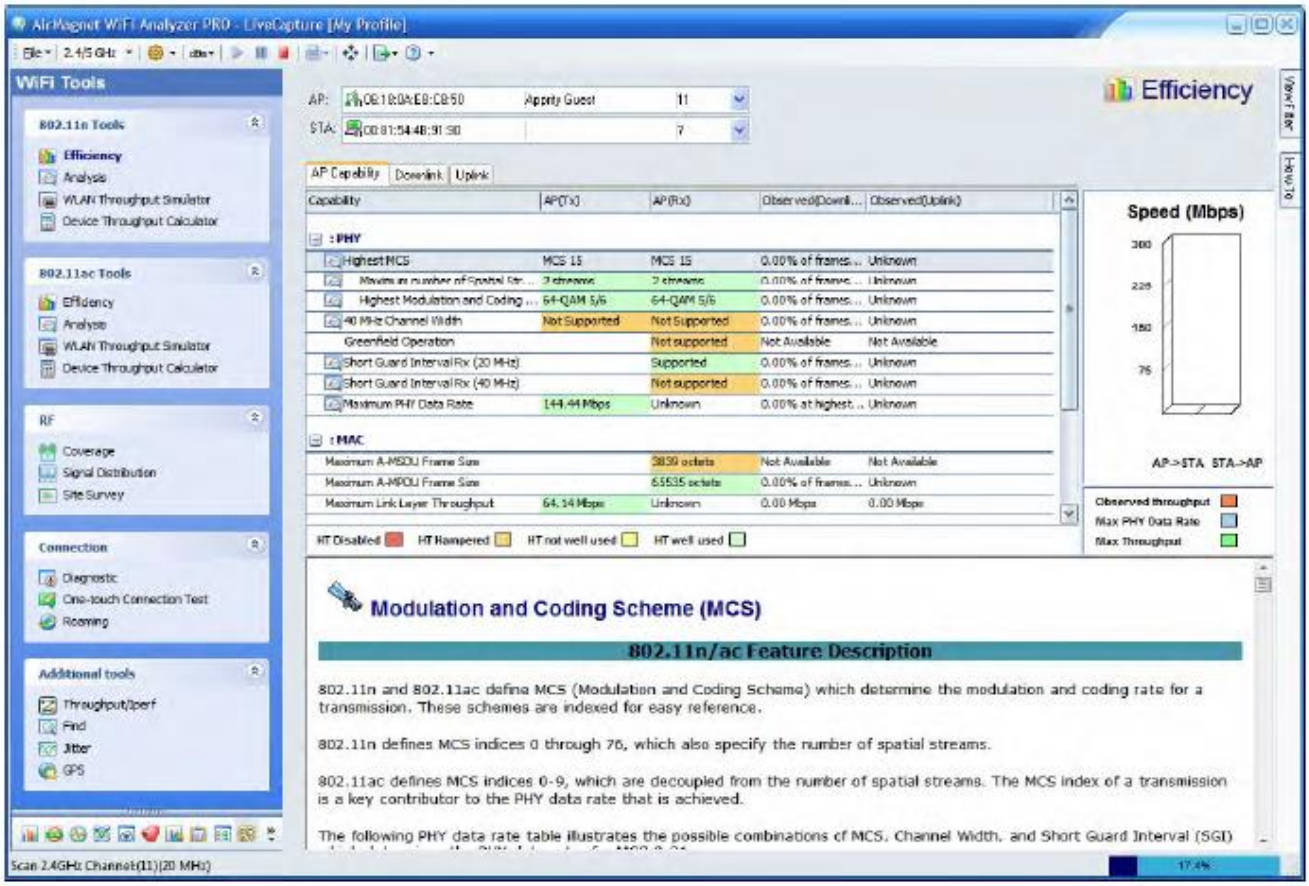
Об инструментах 802.11n/ac

Приложение AirMagnet WiFi Analyzer поставляется с инструментами 802.11n/ac, которые позволяют анализировать производительность беспроводной сети 802.11n/ac – технологии беспроводных сетей нового поколения, обеспечивающей беспрецедентную пропускную способность, дальность действия и стабильность работы. Инструменты предназначены для того, чтобы помочь пользователю понять и устранить наиболее распространенные проблемы, с которыми можно столкнуться на сети 802.11n/ac.
Приложение AirMagnet WiFi Analyzer предоставляет следующие инструменты, относящиеся к 802.11n/ac:

- Efficiency (Эффективность)
- Analysis (Анализ)
- WLAN Throughput Simulator (Моделирование пропускной способности WLAN)
- Device Throughput Calculator (Расчет пропускной способности устройства)

Эффективность 802.11n/ac

Протоколы беспроводной сети 802.11n и 802.11ac вносят существенные улучшения в эффективность работы сети WLAN как на физическом (PHY) уровне, так и на уровне управления доступом к среде (MAC). Инструмент Efficiency предназначен для получения базовой информации, необходимой для полного использования всех преимуществ сетей 802.11n и 802.11ac.



При выборе инструмента Efficiency (Эффективность) на экране WIFI Tools (Инструменты WiFi) отображаются все проблемы, сгруппированные по перечисленным ниже категориям.

- PHY – Охватывает проблемы, связанные с улучшением пропускной способности данных на физическом уровне.
- MAC – Охватывает такие проблемы, связанные с повышением эффективности протокола на уровне управления доступом к среде передачи (MAC), как объединение кадров и подтверждения блоков.
- Coexistence (Сосуществование) – Охватывает проблемы, связанные с обратной совместимостью сети с устаревшими сетями 802.11 (такими как 802.11a/b/g).

Примечание: Двойной щелчок кнопкой мыши на записи обновляет экран до экрана Analysis (Анализ), на котором отображается подробный анализ этой записи (если применимо). Обратитесь к разделу «Анализ эффективности сети 802.11n/ac».

Анализ эффективности сети 802.11n/ac

Инструмент Efficiency позволяет увидеть эффективность сети между любой (выбранной) парой точка доступа – станция или только для точки доступа.

Чтобы проанализировать эффективность сети между точкой доступа и станцией:

1. На экране Efficiency (Эффективность) выберите точку доступа (AP) и станцию (STA).

Примечание: Станция (STA), выделенная жирным зеленым шрифтом в списке STA, является той станцией, которая связана с точкой доступа, выбранной выше в списке AP.

2. Используйте вкладки в верхней части экрана для просмотра различных данных, касающихся эффективности сети между точкой доступа и станцией, как описано в таблице ниже.

Элемент	Описание
Вкладки	Откройте любую из следующих вкладок, чтобы просмотреть соответствующие данные в таблице.
• AP Capability (Возможности точки доступа) • Downlink (Нисходящий канал) • Uplink (Восходящий канал)	Отображает данные только о выбранной точке доступа. Отображает данные о канале от выбранной точки доступа к выбранной станции. Отображает данные о канале от выбранной станции к выбранной точке доступа.
Поля таблицы	
Capability (Возможность)	Перечислены основные функции, которыми обладает устройство 802.11n.
AP (TX) (Точка доступа (передача))	Возможности передачи точки доступа.
AP (Rx) (Точка доступа (прием))	Возможности приема точки доступа.
AP -> STA (точка доступа – станция)	Возможности нисходящего канала (от точки доступа к станции).
STA -> AP (станция – точка доступа)	Возможности восходящего канала (от станции к точке доступа).
Observed (Downlink) (Наблюдаемое (нисходящий канал))	Уровень или состояние определенной возможности, наблюдаемое на нисходящем канале (от точки доступа к станции).
Observed (Uplink) (Наблюдаемое (восходящий канал))	Уровень или состояние определенной возможности, наблюдаемое на восходящем канале (от станции к точке доступа).
Цвета легенды	
Режим HT или VHT отключен	Для столбцов AP (Tx) и AP (Rx) красный цвет означает, что режим HT или VHT отключен или не используется.
Передача HT или VHT затруднена	Для столбцов AP (Tx) и AP (Rx) оранжевый цвет означает, что передача HT или VHT нарушена.
Передача HT или VHT не очень хорошо используется	Для столбцов AP (Tx) и AP (Rx) желтый цвет означает, что возможности HT или VHT используются только на 50 ~ 75%.
Передача HT или VHT хорошо используется	Для столбцов AP (Tx) и AP (Rx) красный цвет означает, что режим HT или VHT используется почти на полную мощность.

3. Обратите внимание на различные скорости передачи данных для нисходящего канала (AP -> STA) слева и для восходящего канала (STA -> AP) справа на гистограмме, как описано в таблице ниже.

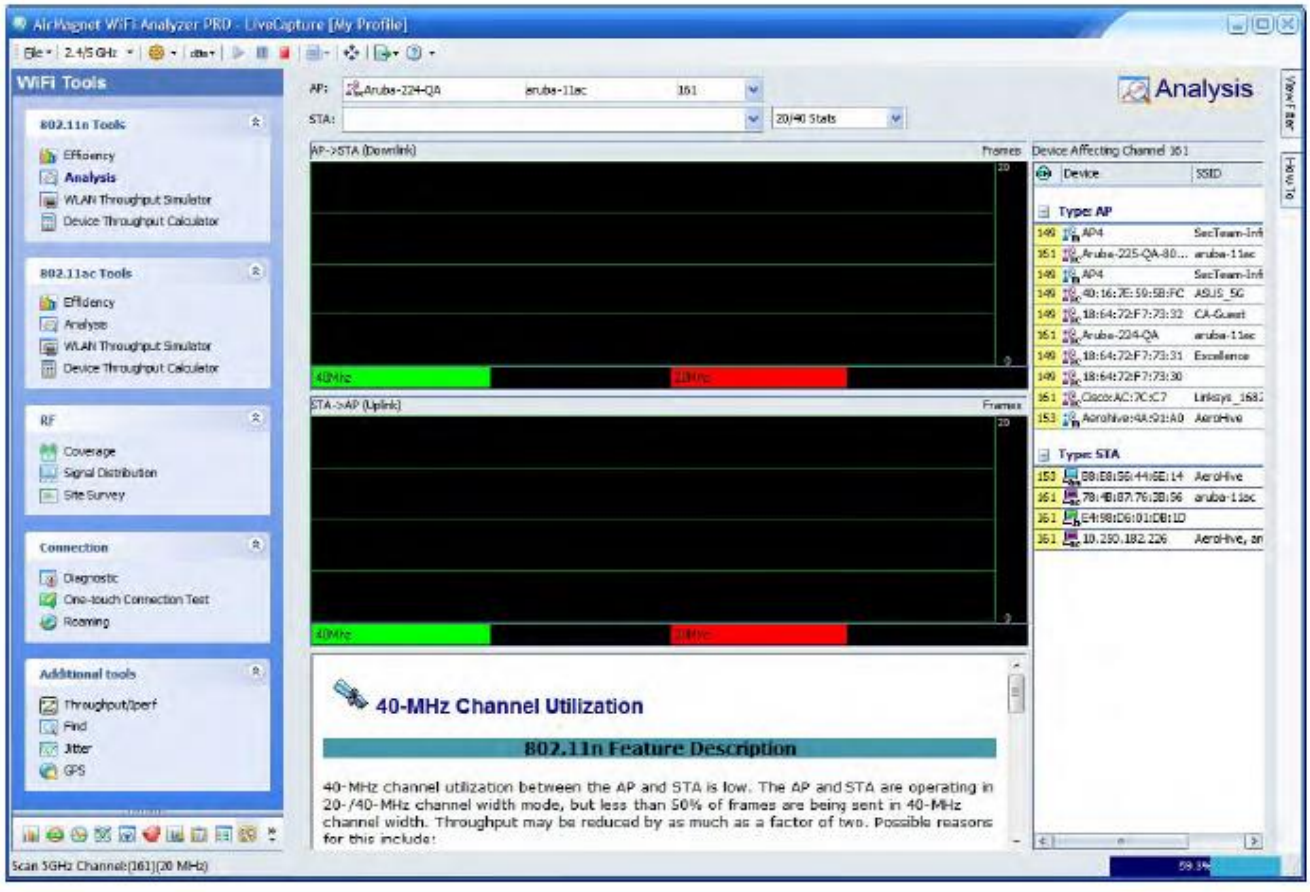
Данные	Описание
Левая гистограмма	Скорость передачи данных по нисходящему каналу (AP -> STA).
Правая гистограмма	Скорость передачи данных по восходящему каналу (STA -> AP).
Цветовая легенда гистограммы	
Светло-зеленый	Максимальная пропускная способность
Голубой	Максимальная скорость передачи данных на физическом уровне (PHY)
Коричневый	Наблюдаемая пропускная способность

В столбцах Observed (Downlink) (Наблюдаемое (нисходящий канал)) и Observed (Uplink) (Наблюдаемое (восходящий канал)) отображается любое из следующего в зависимости от ситуации:

- Когда для пары AP-STA (точка доступа – станция) известно, что она установлена приложением AirMagnet WiFi Analyzer, столбец Observed (Наблюдаемое) содержит показания, специфичные для определенного соединения AP-STA (то есть отображает только измерения трафика, сделанные между комбинацией точки доступа и станции).
- Если не известно, что пара AP-STA связана, в столбце Observed (Наблюдаемое) содержатся показания, которые не зависят от какого-либо соединения (т.е. отображаются все показания исходящего трафика [данных] от точки доступа и станции).
- Когда выбрана точка доступа и «любая» станция, используются показания исходящего трафика (данные) точки доступа, а показания станции (и, следовательно, восходящего канала) равны нулю (то есть никакой трафик не указывается). В этом случае возможности точки доступа сравниваются с «виртуальной» станцией, параметры которой заданы в нормах спецификации 802.111n.

Анализ 802.11n/ac

На экране Analysis (Анализ) представлен подробный анализ (объяснение) ряда проблем, связанных со стандартами 802.11n или 802.11ac. Чтобы перейти к экрану инструментов анализа, щелкните кнопкой мыши на Analysis (Анализ) под 802.11n Tools или 802.11ac Tools. На рисунке ниже показан экран 802.11n Tools/Analysis (Инструменты/Анализ 802.11n).

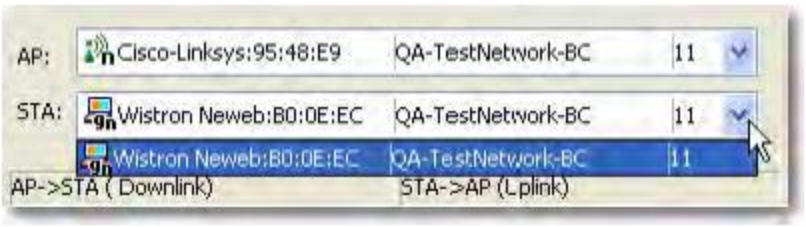


Анализ сетевых данных 802.11n и 802.11ac

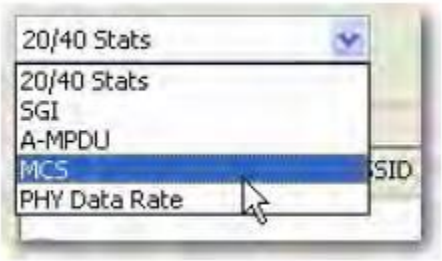
Инструмент Analysis (Анализ) позволяет увидеть следующие сетевые данные 802.11n и 802.11ac между любой (выбранной) парой точка доступа – станция или только для точки доступа:

- Статистика 20/40/80 МГц
- Короткий защитный интервал (SGI)
- A-MPDU
- MCS
- Скорость передачи данных на физическом (PHY) уровне

Для анализа сетевых транзакций между точкой доступа и станцией:



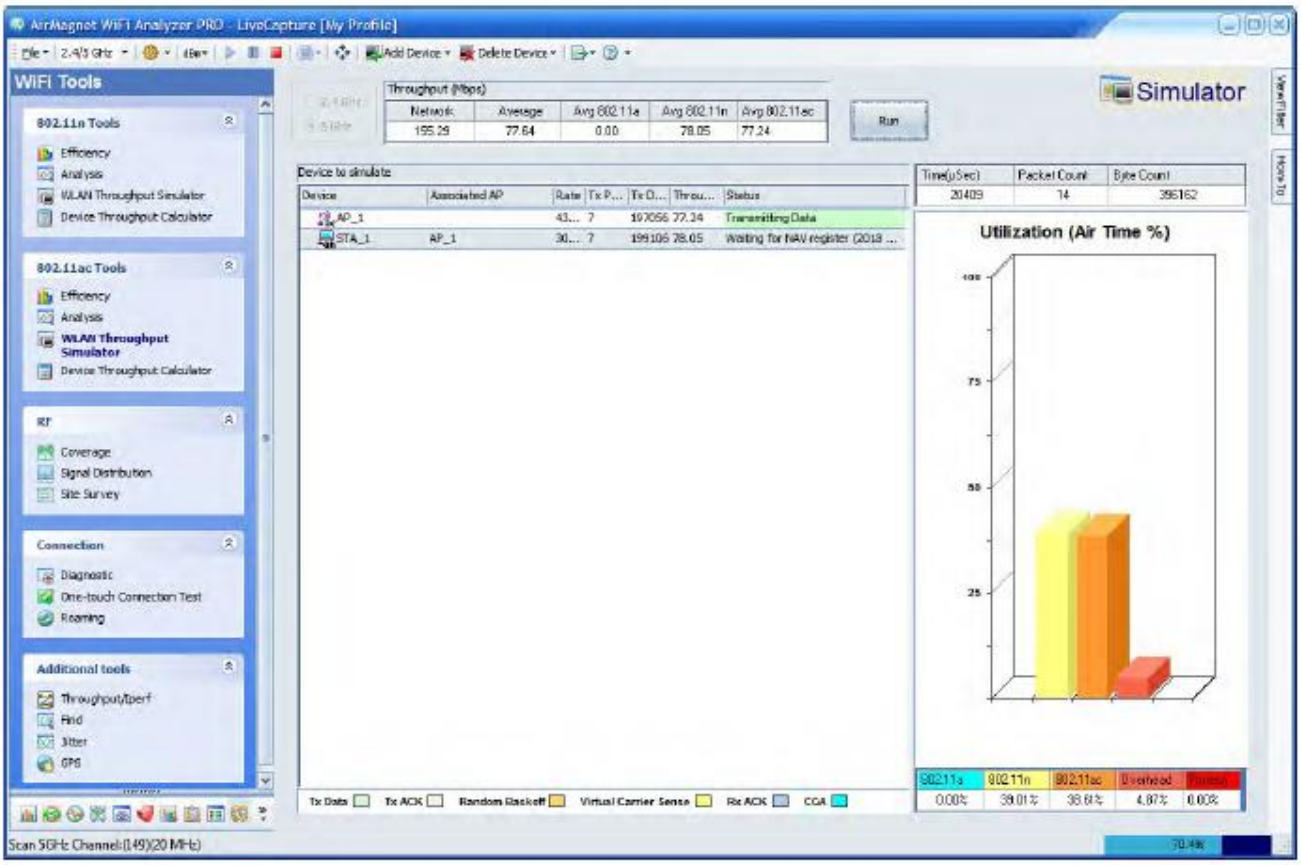
1. На экране WiFi Tools (Инструменты WiFi) щелкните кнопкой мыши на Analysis (Анализ) в разделе 802.11n Tools (Инструменты 802.11n) или 802.11ac Tools (Инструменты 802.11ac).
2. Выберите точку доступа и станцию.
3. Выберите интересующий тип данных.



4. Используйте гистограммы для наблюдения за нисходящим каналом (AP -> STA) и восходящим каналом (STA -> AP).
5. Прочитайте описание внизу в средней части экрана.
6. В правой части экрана просмотрите список устройств, влияющих на выбранный канал.

WLAN Throughput Simulator (Моделирование пропускной способности WLAN)

WLAN Throughput Simulator (Моделирование пропускной способности WLAN) является утилитой расчета пропускной способности, использования и потока служебных данных (измеренных на канальном уровне 802.11) для сети, узла и среды передачи при различных конфигурациях сети и узла. Моделирование позволяет добавлять и настраивать до пятидесяти узлов 802.11a, 802.11b, 802.11g, 802.11n и/или 802.11ac на «виртуальном канале». Механизм моделирования применяет дополнительные параметры сети и узлов в зависимости от типа и настроек присутствующих узлов. Моделирование работает в «идеальной» среде, предполагая, что все узлы могут «слышать» друг друга (что исключает возможность коллизий пакетов и повторных попыток передачи кадров) и что все узлы передают столько (и так быстро), сколько они могут (на основе их индивидуальных и общих параметров сети). Результат такого моделирования дает базовое измерение (в определенной степени теоретическое) максимальной пропускной способности канального уровня, которая может быть достигнута для конкретной конфигурации.

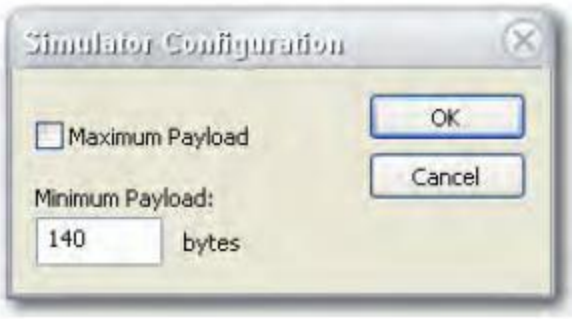


Настройка утилиты WLAN Throughput Simulator

Перед использованием утилиту WLAN Throughput Simulator можно настроить таким образом, чтобы инструмент мог лучше всего моделировать желаемую пропускную способность WLAN.

Для настройки моделирования пропускной способности сети WLAN:

1. На экране WLAN Throughput Simulator щелкните кнопкой мыши на  и выберите в разворачивающемся меню Configure Simulator… (Настроить моделирование). Откроется диалоговое окно Simulator Configuration.



2. Поставьте метку в поле Maximum Payload (Максимальная полезная нагрузка) или укажите минимальный размер пакета.
3. Нажмите кнопку ОК.

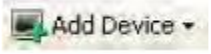
Примечание: Если в поле Maximum Payload (Максимальная полезная нагрузка) установлена метка, утилита будет моделировать состояние, при котором все узлы будут передавать пакеты максимально возможного размера. В противном случае утилита WLAN Throughput Simulator будет моделировать пропускную способность сети WLAN, используя значение полезной нагрузки между заданной минимальной и максимальной полезной нагрузкой (Minimum Payload и Maximum Payload), которое зависит от протокола 802.11, используемого на устройствах. Согласно спецификациям IEEE 802.11n, максимальная передаваемая полезная нагрузка составляет до 2,3 КБ для устройств 802.11a/b/g и 65 КБ для устройств 802.11n, если включен блок данных протокола MAC (MPDU). Максимальная полезная нагрузка 802.11ac составляет 1 МБ.

Моделирование пропускной способности сети WLAN

WLAN Throughput Simulator (Моделирование пропускной способности сети WLAN) позволяет моделировать пропускную способность WLAN при задаваемых пользователем условиях. Все, что вам нужно сделать, это выбрать точку доступа (AP) и станцию (STA), установить параметры и затем нажать Simulate. Приложение AirMagnet WiFi Analyzer сформирует результаты и отобразит их на экране.

Для использования утилиты WLAN Throughput Simulator (Моделирование пропускной способности сети WLAN):

1. На экране 802.11n Tools (Инструменты 802.11n) щелкните кнопкой мыши на WLAN Throughput Simulator.
2. Выберите соответствующий частотный диапазон, щелкнув кнопкой мыши на переключателе 2,4 ГГц или 5 ГГц.

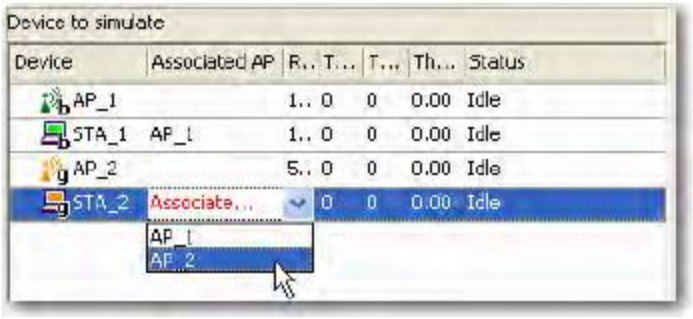
3. На панели меню щелкните кнопкой мыши на 

и выберите нужную опцию в разворачивающемся меню.

Все опции разворачивающегося меню Add Device (Добавить устройство) описываются в таблице ниже.

Опция меню	Описание
Add Existing Device (Добавить существующее устройство)	Позволяет открыть диалоговое окно для выбора и добавления точек доступа и/или станций из списка устройств, обнаруженных на сети WLAN.
802.11a Device (Устройство 802.11a)	Добавляет точку доступа и/или станцию 802.11a.
802.11b Device (Устройство 802.11b)	Добавляет точку доступа и/или станцию 802.11b.
802.11g Device (Устройство 802.11g)	Добавляет точку доступа и/или станцию 802.11g.
802.11n Device (Устройство 802.11n)	Добавляет точку доступа и/или станцию 802.11n.
802.11ac Device (Устройство 802.11ac)	Добавляет точку доступа и/или станцию 802.11ac. Эта опция доступна только для 802.11ac Tools.

4. Свяжите станцию с точкой доступа, щелкнув кнопкой мыши на станции, а затем на направленной вниз стрелке рядом с ней для выбора точки доступа.

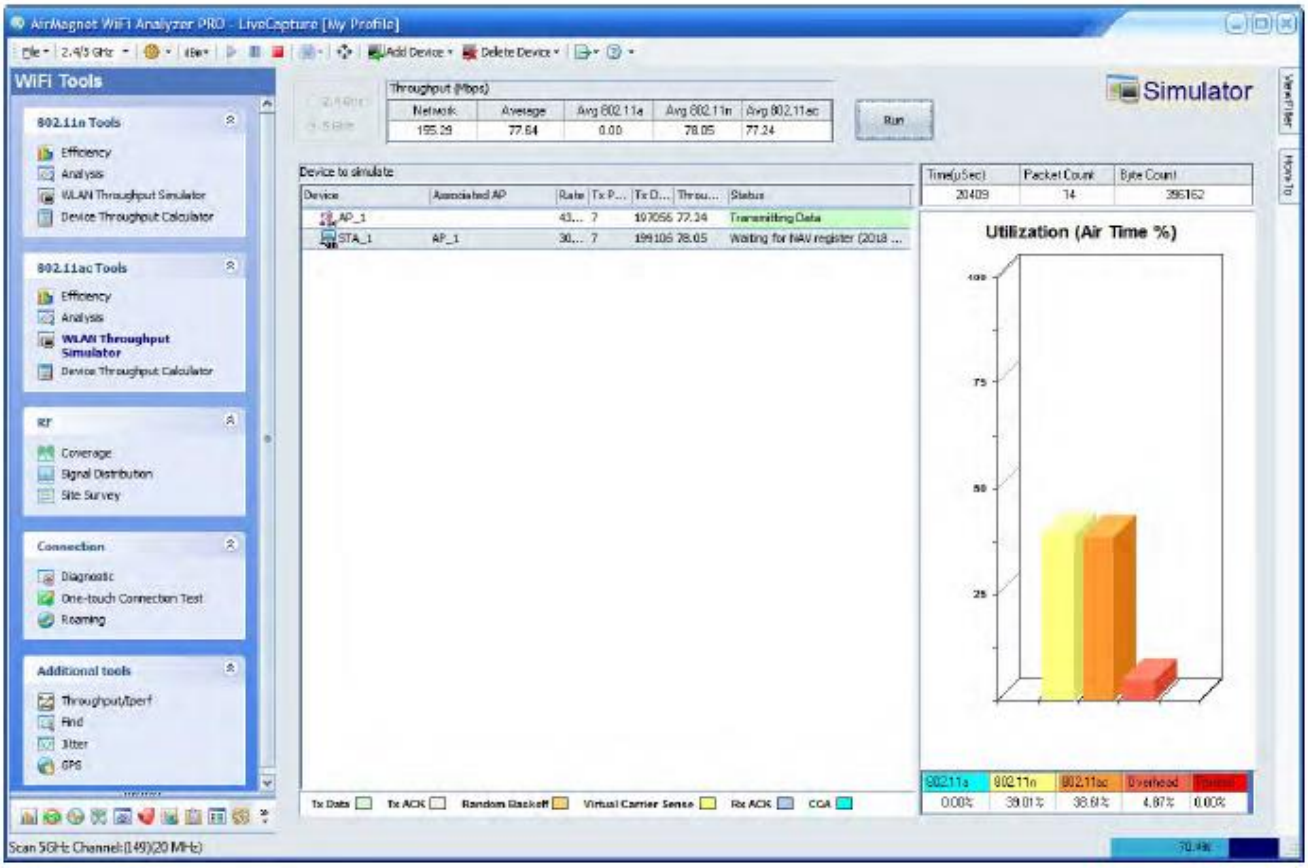


5. Повторите шаг 3 для связи всех точек доступа и станций.

Примечание: Для запуска моделирования пропускной способности WLAN каждая станция должна быть связана с точкой доступа.

6. Нажмите кнопку Run (Выполнить) в правом верхнем углу экрана. Моделирование будет запущено, а результаты будут отображаться на экране.

Смоделированные данные пропускной способности сети WLAN



В приведенной ниже таблице объясняются смоделированные данные WLAN, показанные на экране WLAN Throughput Simulator.

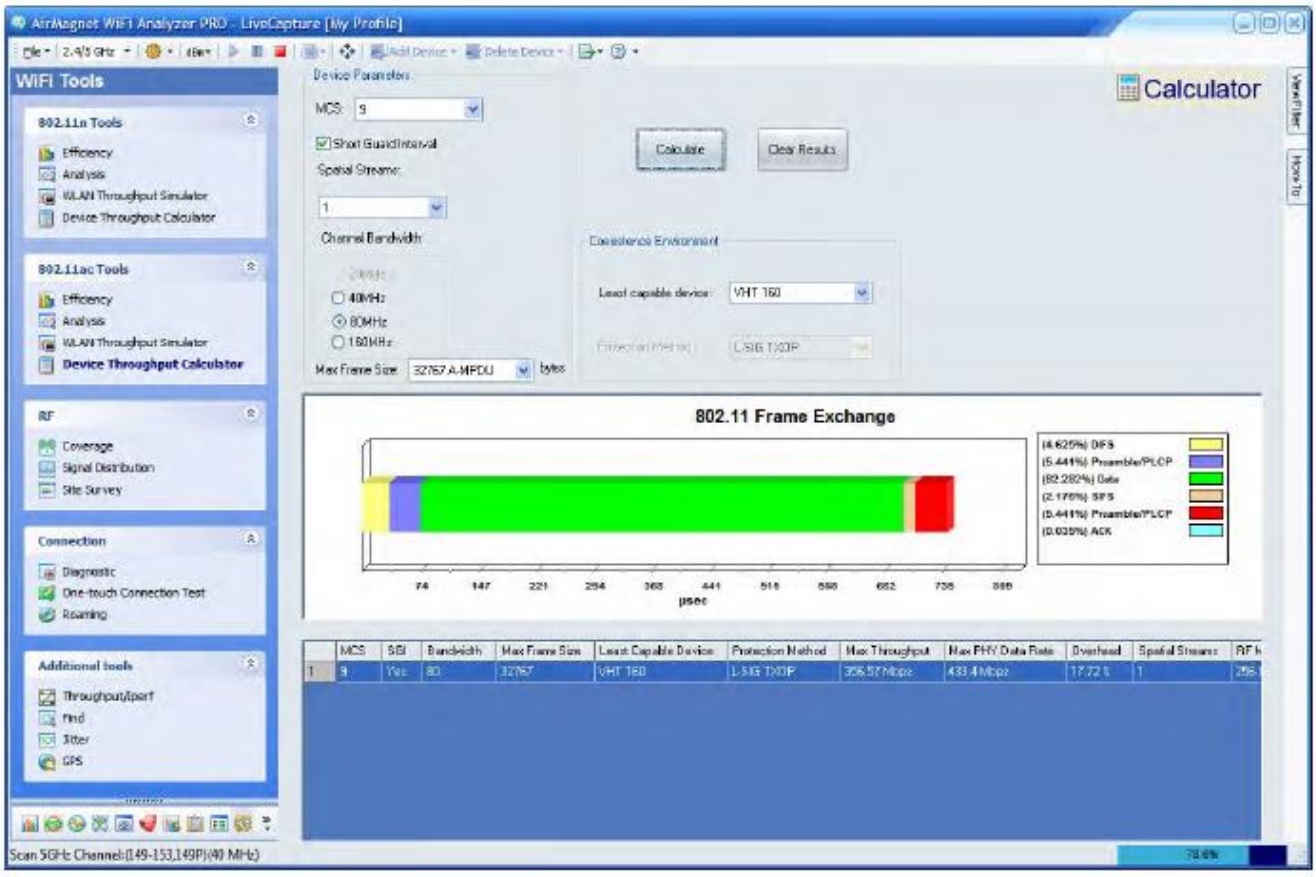
Поле данных	Описание
Throughput (Mbps) (Пропускная способность (Мбит/с))	Отображается пропускная способность сети WLAN в Мбит/с в следующих категориях:
Network (Сеть)	Пропускная способность сети, которая представляет собой объединенную совокупную пропускную способность всех беспроводных сред. В зависимости от того, используете ли вы инструменты 802.11n или 802.11ac, это значение может включать 802.11a/b/g/n/ac, в зависимости от выбранной полосы частот (2,4 ГГц или 5 ГГц).
Average (Средняя)	Средняя пропускная способность узла (когда пропускная способность сети делится на количество узлов).
Avg 802.11a (Средняя для 802.11a)	Средняя пропускная способность узла для всех устройств 802.11a. (Только 5 ГГц).
Avg 802.11b (Средняя для 802.11b)	Средняя пропускная способность узла для всех устройств 802.11b.
Avg 802.11g (Средняя для 802.11g)	Средняя пропускная способность узла для всех устройств 802.11g.
Avg 802.11n (Средняя для 802.11n)	Средняя пропускная способность узла для всех устройств 802.11n.
Avg 802.11ac (Средняя для 802.11ac)	Средняя пропускная способность узла для всех устройств 802.11ac.
Device to Simulate (Устройство для моделирования)	Отображается информация о каждом из устройств, участвующих в моделировании.
Device (Устройство)	Имя или MAC-адрес узла.
Associated AP (Связанная точка доступа)	Имя точки доступа, связанной со станцией или станциями.
Tx Packets (Пакеты передачи)	Количество кадров (пакетов) данных, переданных узлом.
Tx Data Bytes (Байты данных передачи)	Количество байтов данных, переданных узлом.
Rate (Скорость)	Скорость передачи данных физического уровня (PHY Data Rate), используемая узлом для всех передач данных.
Throughput (Пропускная способность)	Пропускная способность отдельных узлов.

Status (Состояние)	Текущее рабочее состояние узлов, которое может быть любым из следующих: • Tx Data • Tx ACK • Random Backoff • Virtual Carrier Sense
Time (µsec) (Время (мкс))	Время моделирования (в мкс). Примечание: Механизм моделирования работает в масштабе времени 1/1000. Это означает, что каждая секунда «реального времени» соответствует миллисекунде «времени моделирования».
Packet Count (Количество пакетов)	Количество пакетов, переданных по каналу.
Byte Count (Количество байтов)	Количество байтов, переданных по каналу.

Примечание: Утилита WLAN Throughput Simulator по-прежнему будет использовать необходимую защиту для передачи на станции 802.11b, даже если настроена для работы в режиме Greenfield, что может быть правильным или неправильным. Кто-то может возразить, что если кто-то устанавливает точку доступа Greenfield, она все еще может позволить станции 802.11b подключиться, а затем перестает использовать режим Greenfield. Пока мы не увидим точку доступа, которая не разрешает подключение, это может быть наиболее близко к тому, что произойдет с реальными точкой доступа и станциями.

Device Throughput Calculator (Расчет пропускной способности устройства)

Device Throughput Calculator – это утилита для расчета теоретической пропускной способности устройства. Просто щелкните кнопкой мыши, чтобы указать такие параметры, как индекс MCS, SGI, пропускная способность, максимальный размер кадра, ACK для блока, наименее работоспособное устройство и/или используемый механизм защиты, и AirMagnet за считанные секунды рассчитает максимальную скорость физического уровня (PHY), максимальную скорость передачи данных, процент служебных данных, количество пространственных кадров и кодовую скорость модуляции. Также данные обмена кадрами 802.11 будут показаны на графике, отображающем процентное соотношение кадров DIFS, преамбулы/PLCP, данных, SIFS, преамбулы/PLCP и ACK. Обратитесь к разделу «Расчет пропускной способности устройства».



Расчет пропускной способности устройства

Утилита Device Throughput Calculator (Расчет пропускной способности устройства) позволяет рассчитать максимальный уровень пропускной способности устройства на основе задаваемых пользователем параметров и условий сосуществования. Результаты всех расчетов можно сохранить на экране. Они позволят получить быструю справочную информацию по уровню производительности, которой сможет достигать устройство в различных условиях.

Для использования утилиты Device Throughput Calculator:

1. На экране WiFi Tools (Инструменты WiFi) щелкните кнопкой мыши на Device Throughput Calculator.
2. На экране Device Throughput Calculator сделайте выбор, как описано в таблице ниже.

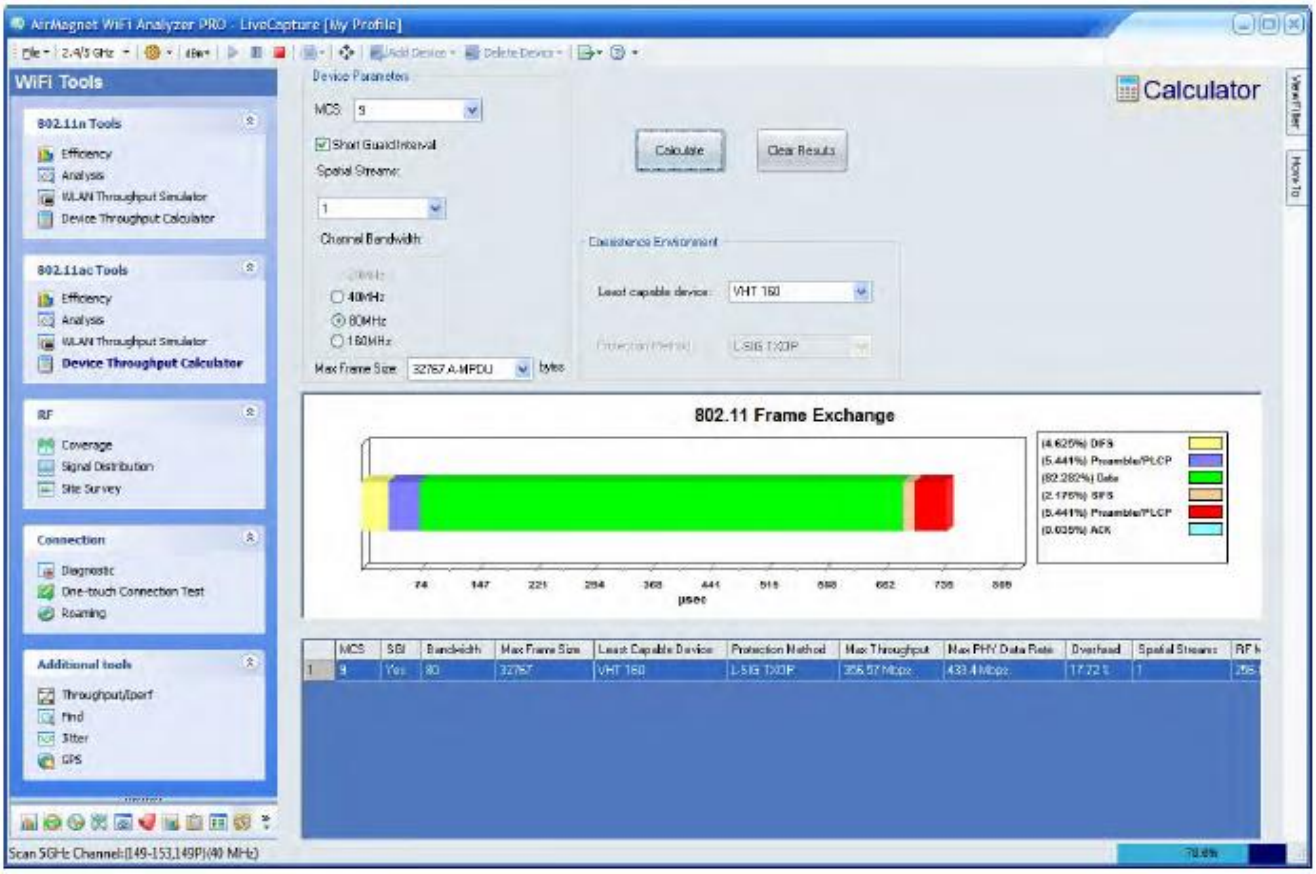
Параметр	Описание
MCS	Щелкните кнопкой мыши на направленной вниз стрелке и выберите опцию из разворачивающегося списка. 802.11n: Каждая схема модуляции и кодирования (MCS) связана с определенным количеством пространственных потоков, а также скоростью модуляции и кодирования, как указано значениями в скобках. 802.11ac: В разворачивающемся списке доступны MCS 1 - 9.
Spatial Streams (902.11ac) (Пространственные потоки (802.11ac))	Щелкните кнопкой мыши на направленной вниз стрелке и выберите опцию из разворачивающегося списка. Эта опция используется в сочетании с MCS.
Short Guard Interval (Короткий защитный интервал)	Если в этом поле стоит метка, включен короткий защитный интервал (Short Guard Interval - SGI).
	Примечание: Когда включена функция SGI, на каналах 20 и 40 МГц для каждой схемы модуляции и кодирования (MCS) скорость передачи данных физического уровня PHY (в Мбит/с) увеличивается приблизительно на 11%.
Channel Bandwidth (Пропускная способность канала)	Выберите желаемую полосу пропускания: 20, 40, 80, 160.
Max Frame Size (Максимальный размер кадра)	Щелкните кнопкой мыши на направленной вниз стрелке и выберите опцию в разворачивающемся списке.
Block ACK (802.11n) (Подтверждение блока)	Если в этом поле стоит метка, используется функция подтверждения блоков.
Last Capable Device (Наименее способное устройство)	Щелкните кнопкой мыши на направленной вниз стрелке и выберите опцию в разворачивающемся списке: • VHT 160 • VHT 80 • VHT 40 • VHT 20 • HT 40 Mixed Mode • HT 20 Mixed Mode • 802.11a
Protection Method (Метод защиты)	Щелкните кнопкой мыши на направленной вниз стрелке и выберите опцию в разворачивающемся списке: • CTS-to-Self • RTS/CTS • L-SGI TXOP
	Примечание: Ни один из этих методов защиты не применяется к HT 40 Greenfield.

3. Нажмите Calculate (Рассчитать). Приложение AirMagnet WiFi Analyzer начнет расчет пропускной способности устройства на основе заданных пользователем параметров, отображая результат на экране.
4. Повторите шаги 2 и 3 для проведения дополнительных расчетов с использованием различных комбинаций параметров.

Примечание: Приложение AirMagnet WiFi Analyzer производит расчет при каждом нажатии кнопки Calculate. Все результаты будут отображаться на экране, что упростит сравнение производительности устройства в различных условиях.

Данные расчета пропускной способности устройства

Приложение AirMagnet WiFi Analyzer рассчитывает данные о пропускной способности устройства на основе параметров, выбранных пользователем, и отображает результаты в нижней половине экрана. На экране отображается информация двух типов: 802.11 Frame Exchange (Обмен кадрами 802.11) на графике и данные о пропускной способности в таблице, как показано на рисунке ниже.



В приведенной ниже таблице кратко объясняется обмен кадрами 802.11, показанный на графике.

Данные	Описание
DIFS	Межкадровый промежуток DCF.
Preamble/PLCP	Преамбула/Процедура конвергенции физического уровня.
Data	Кадр данных.
SIFS	Короткий межкадровый промежуток.
Preamble/PLCP	Преамбула/Процедура конвергенции физического уровня.
ACK	Кадр подтверждения.

Радиочастотные инструменты

О радиочастотных инструментах

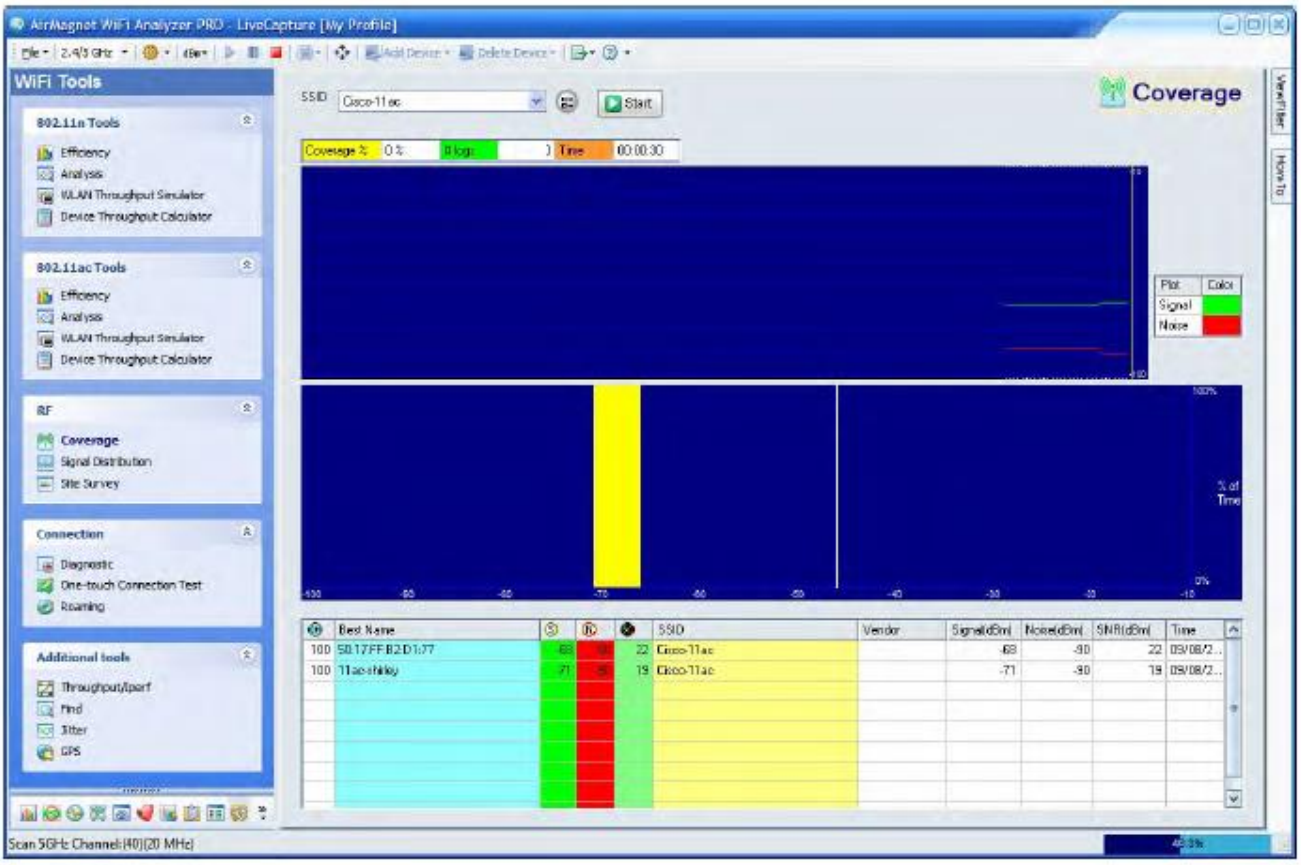
Приложение AirMagnet WiFi Analyzer предоставляет радиочастотные инструменты, которые помогают администраторам сети изучать и понимать радиочастотные условия в месте развертывания их сети WLAN или вокруг нее с точки зрения радиочастотного покрытия, распределения сигнала, мощности сигнала, уровня шумов и т.д. Полученные с помощью этих инструментов реальные радиочастотные данные помогают принимать обоснованные решения относительно развертывания и расширения сети WLAN.

К этой категории относятся три инструмента:

- Coverage (Покрытие): Измеряет зону покрытия радиосигнала в сети WLAN или соте этой сети.
- Signal Distribution (Распределение сигнала): Анализирует характер распределения радиочастотного сигнала.
- Site Survey (Обследование объекта): Собирает радиочастотные данные на площадке WLAN.

Инструмент Coverage (Покрытие)

Инструмент Coverage (Покрытие) предназначен для оценки покрытия радиосигнала в беспроводной сети. Он способен помочь в анализе сетей до или после их развертывания.
Перемещаясь по границам соты во время анализа радиочастотной среды сети, можно будет увидеть покрытие сигнала. При этом вы получите файл журнала, содержащий ценные данные, которые можно использовать в качестве основы для настройки размера радиочастотной соты (ячейки) сети, при котором обеспечивается требуемое покрытие. На рисунке ниже показан экран инструмента Coverage (Покрытие). Также обратитесь к разделам «Настройка инструмента Coverage (Покрытие)» и «Измерение покрытия площадки WLAN».



Настройка инструмента Coverage (Покрытие)

Перед началом тестирования покрытия сигнала, возможно, потребуется настроить некоторые параметры. Это гарантирует получение нужных данных.

Для настройки параметров теста покрытия сигнала:

1. На экране WiFi Tools > Coverage (Инструменты WiFi > Покрытие) щелкните кнопкой мыши на  (Настроить).

2. Сделайте желаемый выбор и нажмите кнопку OK.

Измерение покрытия площадки WLAN

Для измерения покрытия объекта радиочастотным сигналом:

1. В верхней части экрана инструмента Coverage (Покрытие) щелкните кнопкой мыши на направленной вниз стрелке и выберите SSID из разворачивающегося списка.
2. Нажмите 

. Данные начнут появляться на экране.

3. Чтобы завершить тестирование покрытия, нажмите Stop.

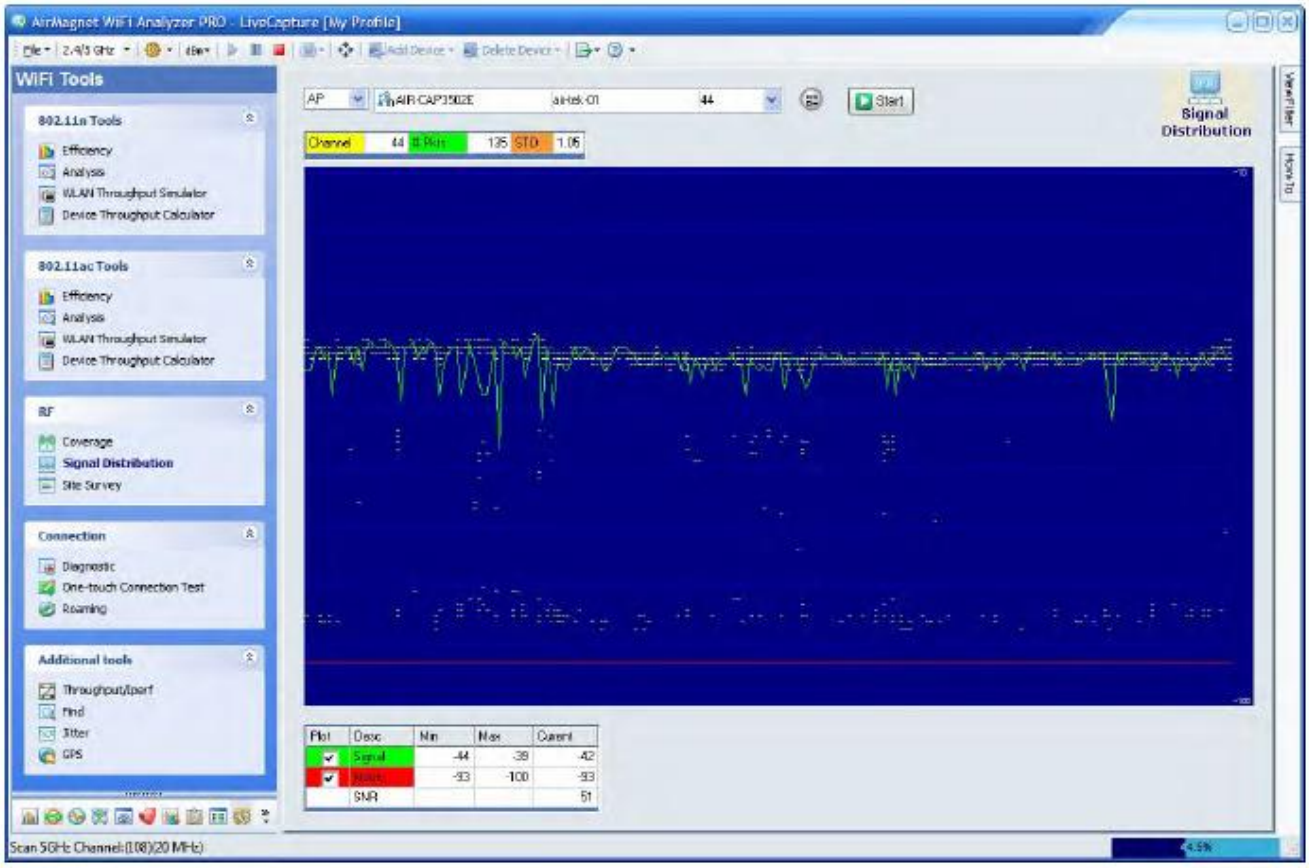
Экран инструмента Coverage (Покрытие) предоставляет полную картину покрытия радиосигнала для выбранного идентификатора SSID. Инструмент также показывает объем трафика, превышающий заданный минимальный уровень обслуживания (Minimum Service Level), который представлен на гистограмме белой вертикальной линией. Полосы справа от белой линии представляют точки доступа, уровень сигнала которых соответствует минимальному уровню обслуживания или превышает его, а полосы слева от белой линии представляют точки доступа, уровень сигнала которых ниже минимального уровня обслуживания. На рисунке выше показано, что 86% SSID имеет необходимое покрытие, когда минимальный уровень обслуживания установлен на 60%.

Если для покрытия объекта настроены три точки доступа, можно взять приложение AirMagnet WiFi Analyzer и перемещаться по зоне покрытия. Просматривая уровни сигналов всех точек доступа, можно либо отрегулировать мощность их передачи, либо перемещать точки доступа для обеспечения достаточного или оптимального покрытия радиочастотного сигнала.

Инструмент Signal Distribution (Распределение сигнала)

Инструмент Signal Distribution (Распределение сигнала) предназначен для обнаружения таких проблем с радиочастотным сигналом, как многолучевое распространение. Он позволяет легко отслеживать диаграммы распределения радиосигнала на сети WLAN и визуализировать проблемы, которые в противном случае было бы трудно увидеть и проанализировать. Ниже приводится пример экрана

инструмента Signal Distribution. Также обратитесь к разделам «Настройка инструмента Signal Distribution (Распределение сигнала)» и «Тестирование распределения сигналов на площадке WLAN».



Настройка инструмента Signal Distribution (Распределение сигнала)

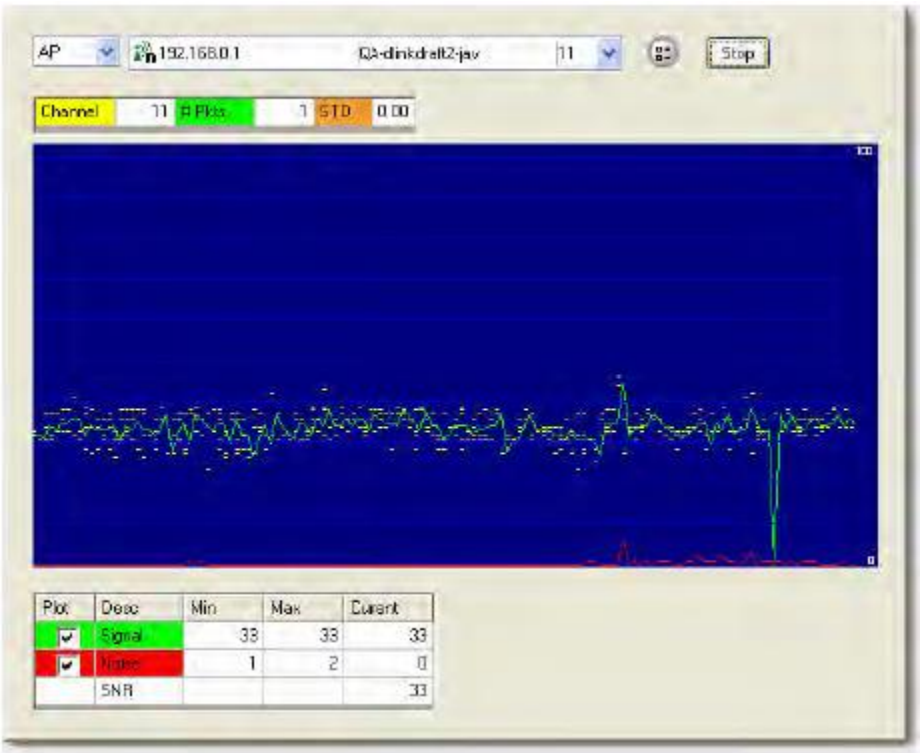
Для настройки параметров инструмента Signal Distribution (Распределение сигнала):

1. На экране WiFi Tools > Signal Distribution (Инструменты WiFi > Распределение сигнала) щелкните кнопкой мыши на  (Опции ведения журнала).
2. Сделайте желаемый выбор и нажмите кнопку OK.

Тестирование распределения сигналов на площадке WLAN

Для проведения теста распределения сигнала:

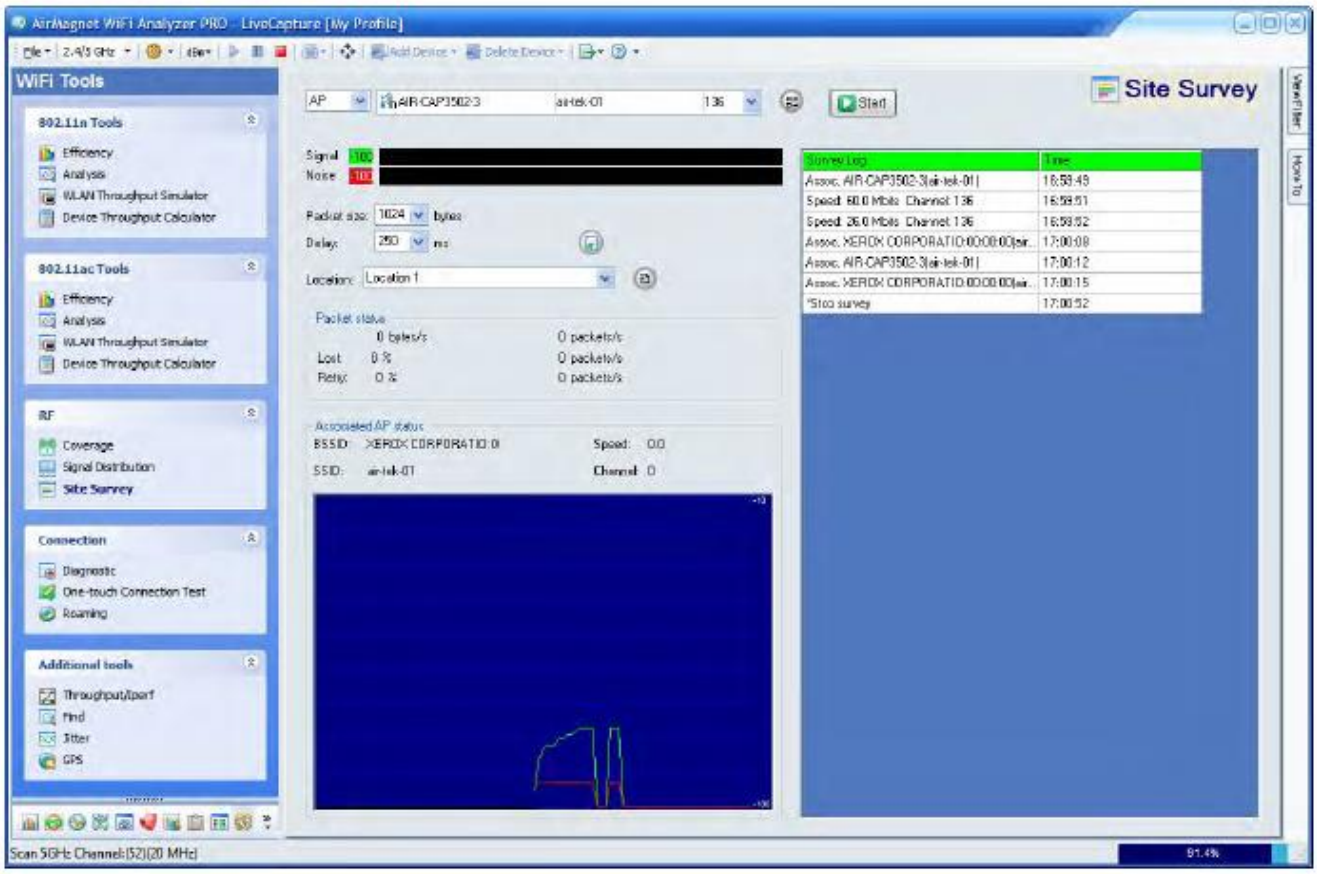
1. На экране Tools > Signal Dist (Инструменты > Распределение сигнала) выберите AP (Точка доступа) или STA (Станция), а затем выберите конкретную точку доступа или станцию справа.
2. Нажмите Start. На экране начинают появляться данные о распределении сигнала.
3. Для завершения теста нажмите Stop.



Примечание: Показанная в приведенном выше примере группа желтых точек представляет собой радиочастотный сигнал для каждого пакета, видимый из текущего местоположения. В случае хорошего распределения сигнала все точки должны находиться близко друг к другу в узком диапазоне. Это означает, что радиочастотные сигналы на площадке имеют одинаковый уровень с небольшими отклонениями. С другой стороны, если точки разбросаны по всему экрану, значит, мощность сигнала меняется, и, возможно, существует проблема, которая требует вашего внимания.

Инструмент Site Survey (Обследование площадки)

Инструмент Site Survey (Обследование площадки) обеспечивает углубленную проверку и анализ радиочастотных условий на предполагаемой или существующей площадке развертывания сети WLAN. Основная цель обследования площадки - убедиться, что беспроводные станции принимают хороший радиосигнал и имеют необходимую скорость передачи в зоне их работы, а также определить количество точек доступа, необходимых для покрытия зоны, и оптимальные места для их размещения. Тщательное обследование площадки поможет убедиться, что схема и развертывание сети WLAN соответствуют требованиям к зоне покрытия радиочастотного сигнала и пропускной способности сети. Инструмент Site Survey позволяет проводить обследования площадки WLAN для оценки радиочастотных показателей площадки с точки зрения мощности сигнала, уровня шумов, скорости передачи и т.д. прямо из приложения AirMagnet WiFi Analyzer. В приведенном ниже примере показан экран инструмента Site Survey (Обследование площадки) приложения AirMagnet WiFi Analyzer. Также смотрите разделы «Настройка инструмента Site Survey (Обследование площадки)» и «Проведение обследования площадки WLAN».



Встроенный инструмент Site Survey (Обследование площадки) приложения AirMagnet WiFi Analyzer дополняет программу обследования площадки, которая поставляется с продуктами WLAN, приобретенными у поставщика WLAN. Для изучения всех требований и процедур обследования WLAN изучите руководство по обследованию площадки, предоставляемое производителем вашего оборудования WLAN.

Перед началом сбора данных проекта обследования площадки необходимо получить план или чертеж здания или офиса. Также с помощью простой идентификации необходимо определить место, в котором необходимо получить данные обследования; например, Location 1 (Местоположение 1), Location 2 (Местоположение 2) и т.д.

Настройка инструмента Site Survey (Обследование площадки)

Для настройки инструмента Site Survey:

1. На экране инструмента Site Survey (Обследование площадки) щелкните кнопкой мыши на  (Опции ведения журнала).

2. Укажите путь для экспортирования файла обследования.
3. Введите уникальное имя файла, соответствующее местоположению обследования.
4. Уберите метку из поля Trigger by event (Запуск по событию).
5. Сделайте другой выбор по своему усмотрению.
6. Нажмите кнопку OK.

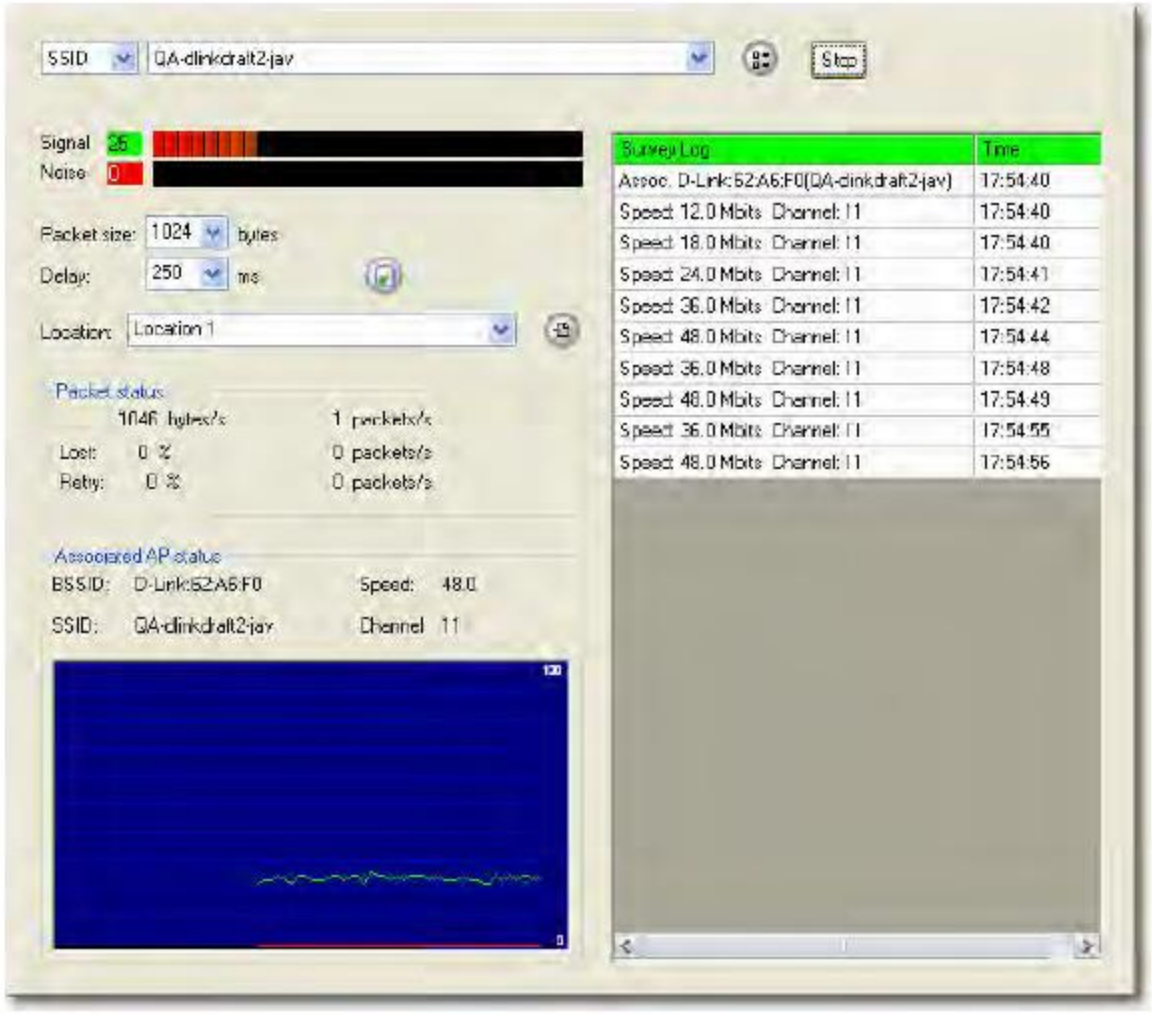
Проведение обследования площадки WLAN

Для проведения обследования площадки WLAN:

1. Пройдите с ноутбуком (на котором запущено приложение AirMagnet WiFi Analyzer) в запланированное местоположение 1 (Location 1).
2. На экране WiFi Tools (Инструменты WiFi) выберите AP или SSID, а затем конкретную точку доступа или идентификатор SSID, с которым хотите установить связь.

3. Нажмите 

. На экране в реальном времени начнут появляться данные.



4. Для завершения обследования нажмите 

.

Настройка управления роумингом

Кнопка  (Опция роуминга) справа от полей Packet Size (Размер пакета) и Delay (Задержка) окна обследования дает возможность управлять состоянием роуминга вашего компьютера. Она позволяет на основе нескольких различных значений указать, как ваш компьютер будет переключаться при перемещении.

Для настройки параметров роуминга в приложении AirMagnet WiFi Analyzer:

1. На экране WiFi Tools > Site Survey (Инструменты Wi-Fi > Обследование площадки) щелкните кнопкой мыши на  . Откроется диалоговое окно Set Roaming Criteria (Установить критерий роуминга).

2. Щелкайте кнопкой мыши на направленных вниз стрелках, чтобы настроить значения сигнала (Signal), скорости (Speed) и максимального числа повторных попыток (Max Retries) для протоколов 802.11 на ноутбуке, когда он переходит в состояние роуминга.

Роуминг начинается при достижении любого из этих значений. Настройка роуминга на основе уровня сигнала заставляет ваш компьютер переключаться, когда достигается определенный минимальный уровень сигнала. Настройка роуминга на основе скорости заставляет его переключаться при достижении минимальной скорости передачи. Максимальное же количество повторных попыток определяет, сколько раз компьютер должен повторно отправлять потерянные данные на точку доступа.

Содержимое диалогового окна Set Roaming Criteria (Установить критерий роуминга) зависит от используемого частотного диапазона (2,4 ГГц или 5 ГГц). Если выбран диапазон 2,4 ГГц, строка 802.11a будет неактивна (не применяется). Если же используется диапазон 5 ГГц, неактивны будут 802.11b и 802.11g.

Примечание: Список адаптеров, поддерживающих эту функцию, можно найти по адресу https://www.netally.com/wp-content/uploads/2019/12/AMM-Preferred-Adapters.pdf. Найдите нужный адаптер и нажмите More details (Подробная информация). Смотрите столбец «Управление роумингом для активных обследований».

Connection (Соединение)

Инструменты анализа соединений WLAN

Приложение AirMagnet WiFi Analyzer предоставляет инструменты для анализа соединений между сетевыми узлами и/или устройствами. Они позволяют сетевому администратору эффективно выявлять и устранять проблемы с сетевыми соединениями.

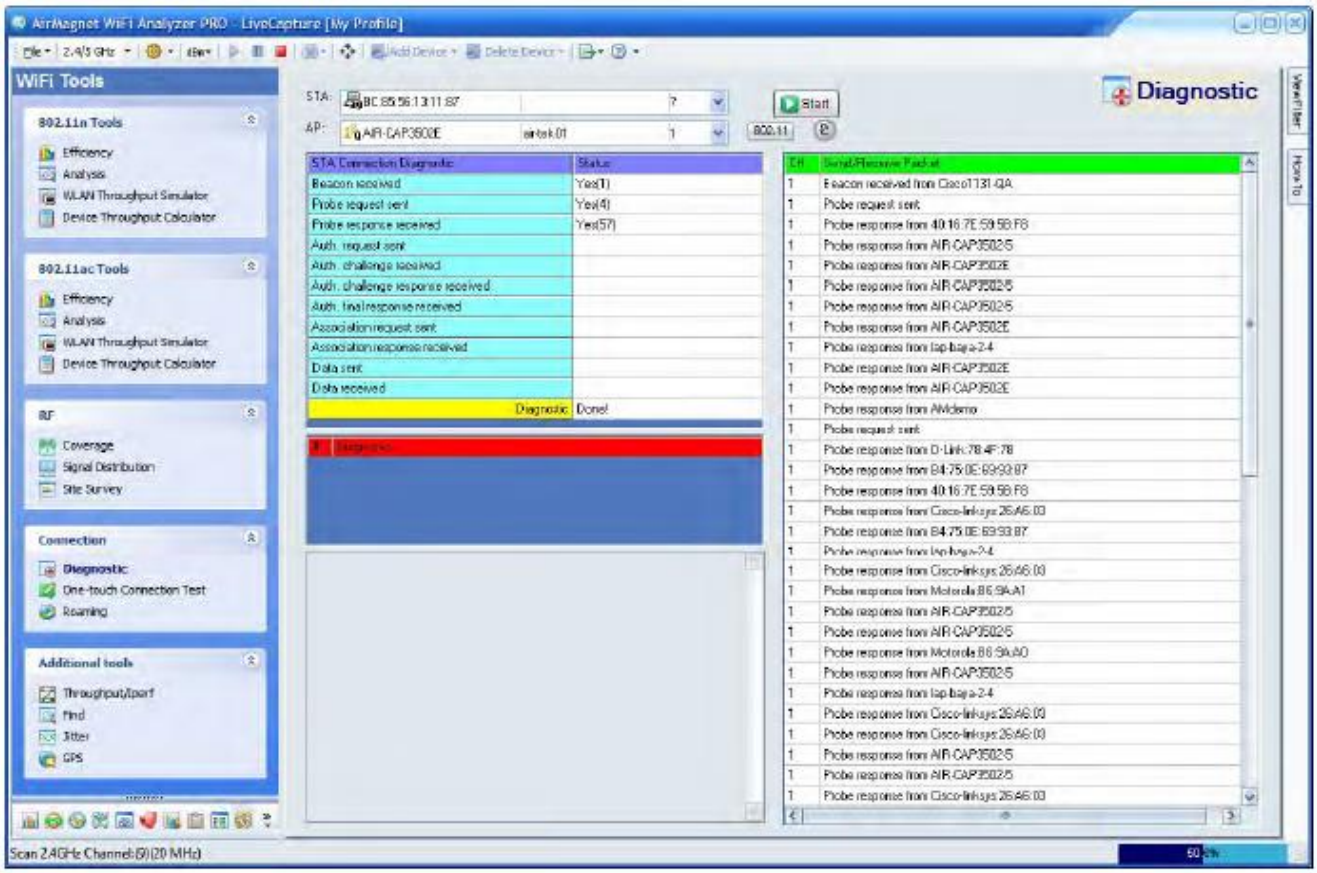
Ниже приведены инструменты для анализа соединений:

- Diagnostic (Диагностика) – Позволяет выявлять несовпадающие конфигурации, такие как SSID, ключи WEP, скорости передачи, преамбулы или радиочастотные каналы.
- One-Touch Connection Test (Тестирование соединения в одно касание) – Позволяет находить и устранять неисправности, и выявлять первопричины любой проблемы с сетевым соединением.
- Roaming (Роуминг) – Позволяет устранять проблемы с роумингом VoWLAN, которые могут вызвать потерю вызовов.

Инструмент Diagnostic (Диагностика)

Без использования интеллектуальных инструментов процесс поиска и устранения проблем с соединением между клиентской станцией и точкой доступа может привести к огромному расходу профессиональных ресурсов. Инструмент Diagnostic (Диагностика) приложения AirMagnet WiFi Analyzer позволяет выявить

несовпадающие конфигурации, такие как SSID, ключи WEP, скорость передачи, преамбулы или радиочастотные каналы. Также он помогает сузить проблему до конкретного этапа процесса подключения, на котором происходит сбой соединения. В число этапов входят обнаружение зондирующих сигналов, аутентификация, повторное соединение и потенциальные сбои оборудования. Экран инструмента Diagnostic (Диагностика) показан на рисунке ниже. Обратитесь также к разделу «Диагностика проблем с сетевым подключением».

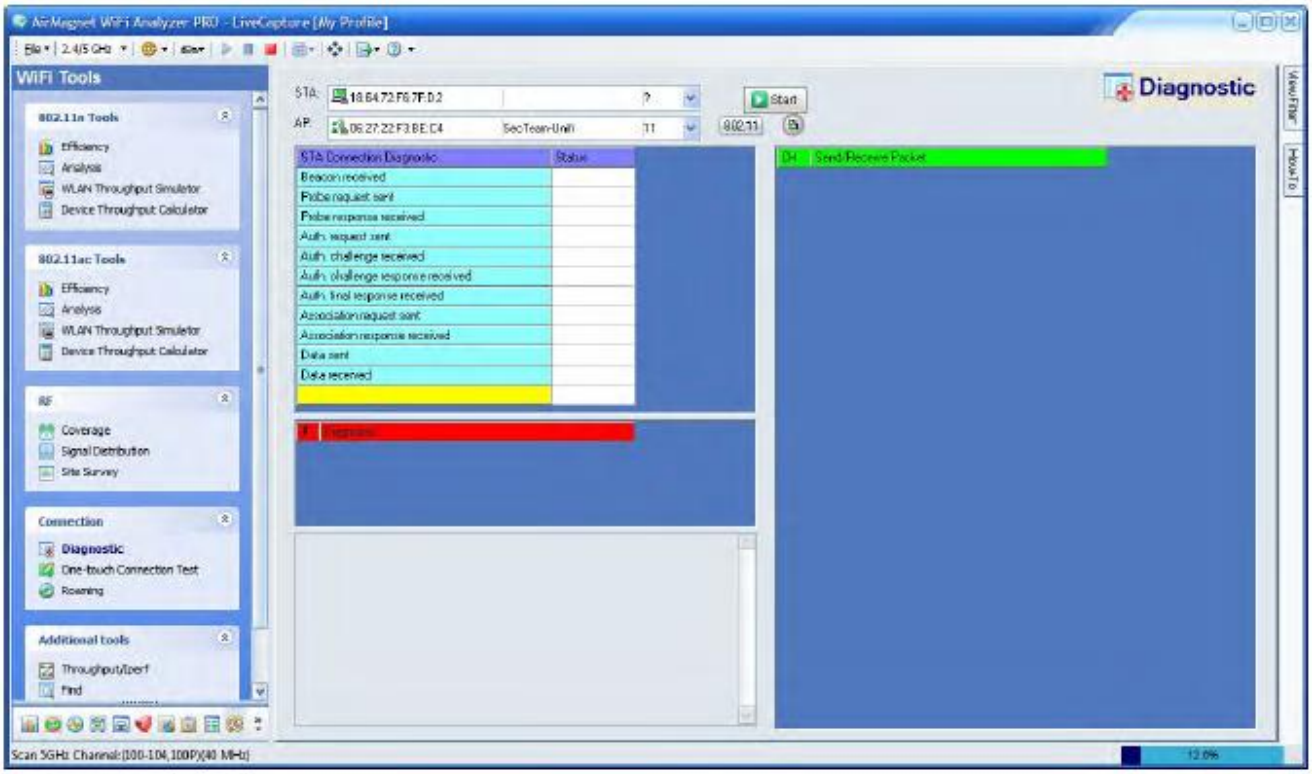


Диагностика проблем с сетевым подключением

Для диагностики проблемы подключения клиентской станции:

1. Найдите MAC-адрес клиентской станции в служебной программе настройки клиента или на задней стороне карты WLAN 802.11.
2. Не выключайте клиентскую станцию.
3. Поместите портативный компьютер (с запущенным приложением AirMagnet WiFi Analyzer) рядом с клиентской станцией.

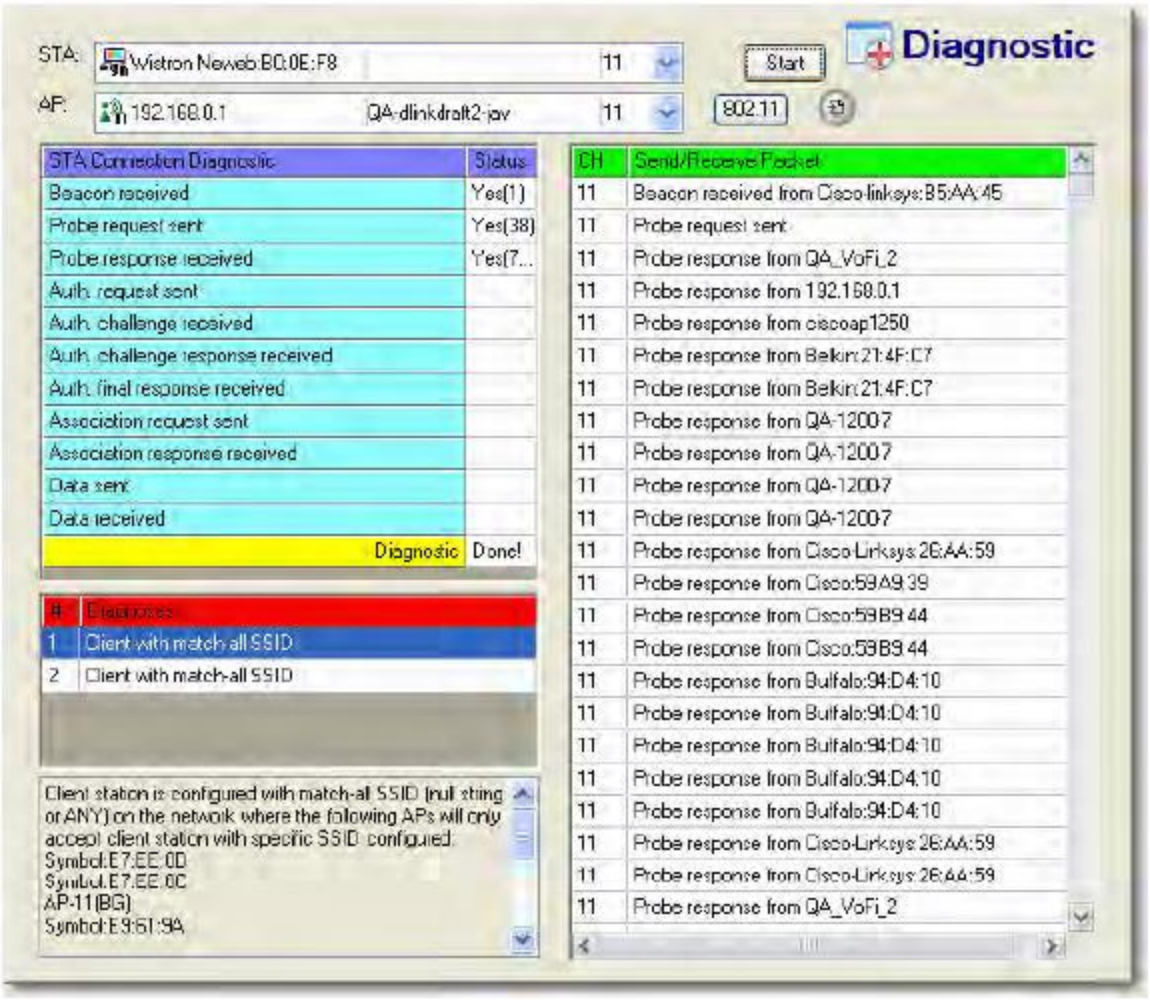
4. На экране WiFi Tools (Инструменты WiFi) щелкните кнопкой мыши на инструменте Diagnostic (Диагностика).



5. Для STA (станция) выберите MAC-адрес клиентской станции в разворачивающемся списке STA.
6. Для AP (точка доступа) выберите точку доступа, к которой должен подключаться клиент, в разворачивающемся списке AP.

Примечание: Если вы не уверены, какую точку доступа нужно использовать, можно выбрать ЛЮБУЮ, но точность диагностики снизится.

7. Нажмите Start. На экране Diagnostic (Диагностика) отобразится процесс соединения с точкой доступа.



Примечание: Диагностический тест автоматически завершается по достижении 100%. Однако, если необходимо остановить выполняемый диагностический тест, просто нажмите Stop.

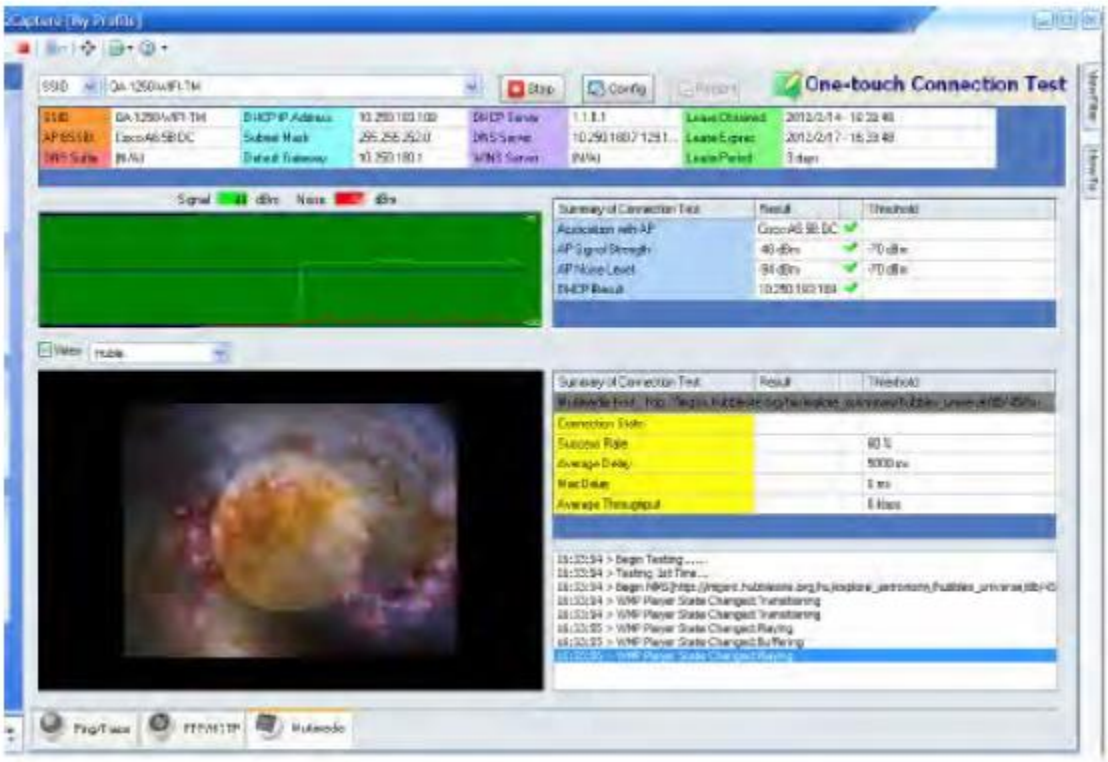
8. Результаты диагностики (в которых указаны предполагаемые причины проблем с соединением и подключением) приводятся в средине и внизу на левой стороне экрана.
9. В правой части экрана приводится пошаговый журнал.
10. Для отображения информации 802.1x нажмите 802.1X.
11. Чтобы экспортировать данные журнала, щелкните кнопкой мыши на (Экспортировать).

Инструмент One Touch Connection Test (Тестирование соединения одним касанием)

Проблемы с подключением в сети WLAN могут возникать из-за неисправности уровня канала передачи данных 802.11 или неправильной конфигурации сетевого уровня IP. Чтобы найти и устранить неисправность и определить основную причину любой проблемы с соединением, необходимо изучить взаимодействие между двумя сетевыми уровнями. Инструмент One Touch Connection Test (Тестирование соединения одним касанием) приложения AirMagnet WiFi Analyzer позволяет легко провести ряд тестов сквозного соединения из одного пользовательского интерфейса.

Приложение AirMagnet WiFi Analyzer предоставляет следующие уникальные интегрированные активные инструменты для устранения подобных неисправностей:

- Ping
- Trace
- FTP
- HTTP
- Multimedia



Настройка

Для настройки инструмента One-Touch Connection Test щелкните кнопкой мыши на Config в верхней части экрана.

Создание отчета

Чтобы создать отчет о результатах работы теста One-Touch Connection Test, перед его запуском необходимо выбрать опцию отчета. Откройте вкладку Report (Отчет) в диалоговом окне Configuration (Конфигурация) и поставьте метку в поле Create One-Touch Connection Test Report (Создать отчет о тестировании соединения одним касанием).

Для добавления в отчет такой информации, как имя отчета (Report Name), местоположение (Location), имя специалиста (Tester Name), верхний и нижний колонтитулы (Page Header и Page Footer) используйте Report Options (Параметры отчета).

После запуска One-Touch Connection Test будут запускаться тесты и собираться информация. Для просмотра отчета после завершения теста нажмите Report.
Форматы отчетов: PDF, HTML, RTF, XLS и XML.

Одновременные сеансы/тесты и несколько мест назначения

Для тестов Ping Test, FTP Test и HTTP(S) Test можно выбрать одновременное выполнение тестов к одному и тому же месту назначения, а также одновременное тестирование нескольких мест назначения.

Concurrent Sessions/Tests (Одновременные сеансы/тесты): Поставьте метку в этом поле, чтобы запустить параллельные (одновременные) сеансы для выбранного теста (например, хоста). Используйте разворачивающийся список справа, чтобы установить количество одновременно запускаемых сеансов (1 - 10). Используйте эту опцию в сочетании с опцией Concurrent Multiple Destinations (Одновременное тестирование нескольких мест назначения).

Concurrent Multiple Destinations (Одновременное тестирование нескольких мест назначения): Если создано несколько тестов (хостов), их можно запускать одновременно. Для этого установите метку в поле Multiple Concurrent Destinations. Данную опцию можно использовать в сочетании с опцией Concurrent Sessions/Tests (Одновременные сеансы/тесты).

Настройка Ping-теста

1. Щелкните кнопкой мыши на Config (Настроить).
2. Откройте вкладку Ping.
3. Нажмите New (Создать) и введите имя теста. Нажмите кнопку ОК.
4. Выбрав имя теста, в текстовое поле Host введите веб-адрес (например, www.domainName.com).
5. При необходимости измените любые другие настройки по умолчанию.

Опция	Описание
Timeout (Таймаут)	Время в миллисекундах до прерывания Ping-теста.
Length (Длина)	Длина кадра в байтах.
#Tests (Количество тестов)	Количество последовательных запусков теста.
Delay (Задержка)	Время задержки между тестами.
Success Rate (Степень успешности)	Процент ответов для успешности теста.
Average RTT (Среднее время двустороннего прохождения)	Среднее время двустороннего прохождения сигнала.
Maximum RTT (Максимальное время двустороннего прохождения)	Максимальное время двустороннего прохождения сигнала.
AP Signal Strength (Мощность сигнала точки доступа)	Уровень сигнала связанной точки доступа.
AP Noise Level (Уровень шума точки доступа)	Уровень шума в дБм.

Настройка теста Trace

Используйте опцию Trace, чтобы изолировать путь трассировки и определить местонахождение неисправности.
1. Щелкните кнопкой мыши на Config (Настроить).
2. Откройте вкладку Trace.
3. Нажмите New (Создать) и введите имя теста. Нажмите кнопку ОК.

4. Выбрав имя теста, в текстовое поле Host введите веб-адрес (например, www.domainName.com).
5. При необходимости измените любые другие настройки по умолчанию.

Опция	Описание
#Tests (Количество тестов)	Количество последовательных запусков теста.
Success Rate (Степень успешности)	Процент ответов для успешности теста.
Average Delay (Средняя задержка)	Средняя задержка на двустороннее прохождение сигнала при обмене данными с хостом в миллисекундах.
Maximum Delay (Максимальная задержка)	Максимальная задержка на двустороннее прохождение сигнала при обмене данными с хостом в миллисекундах.

Настройка FTP

Инструмент FTP позволяет подключаться к указанному серверу FTP и выгружать и загружать выбранный файл столько раз, сколько установлено в конфигурации.

1. Щелкните кнопкой мыши на Config (Настроить).
2. Откройте вкладку FTP.
3. Нажмите New (Создать) и введите имя теста. Нажмите кнопку OK.
4. Выбрав имя теста, введите информацию о сервере FTP.
5. При необходимости измените любые настройки по умолчанию.

Опция	Описание
Server (Сервер)	IP-адрес FTP-хоста.
Port (Порт)	Номер порта для FTP-хоста.
#Tests (Количество тестов)	Количество запусков теста.
User (Пользователь)	Имя пользователя FTP-хоста.
Password (Пароль)	Пароль FTP-хоста.
Local File (Локальный файл)	Путь к файлу, который будет использоваться для выгрузки и загрузки с сервера FTP.
Upload Success Rate (Коэффициент успешной выгрузки)	Процент успешной выгрузки для количества запусков теста.
Upload Average Throughput (Средняя пропускная способность выгрузки)	Требуемая средняя скорость в килобитах в секунду для успешного прохождения теста.
Upload Average Delay (Средняя задержка выгрузки)	Требуемая средняя задержка соединения выгрузки для успешного прохождения теста.
Upload Maximum Delay (Максимальная задержка выгрузки)	Требование к максимальной задержке соединения выгрузки для успешного прохождения теста.
Download Success Rate (Коэффициент успешной загрузки)	Процент успешной загрузки для количества запусков теста.
Download Average Throughput (Средняя пропускная способность загрузки)	Требуемая средняя скорость в килобитах в секунду для успешного прохождения теста.
Download Average Delay (Средняя задержка загрузки)	Требуемая средняя задержка соединения загрузки для успешного прохождения теста.
Download Maximum Delay (Максимальная задержка загрузки)	Требование к максимальной задержке соединения загрузки для успешного прохождения теста.

Настройка HTTP(s)

Инструмент HTTP работает так же, как и инструмент FTP, тестируя выгрузку/загрузку HTTP вместо FTP. Он позволяет подключаться к указанному серверу HTTP и передавать выбранный файл туда и обратно столько раз, сколько требуется для проверки возможности подключения.

1. Щелкните кнопкой мыши на Config (Настроить).
2. Откройте вкладку HTTP.
3. Нажмите New (Создать) и введите имя теста. Нажмите кнопку OK.
4. Выбрав имя теста, введите URL-адрес и имя изображения или файла (или скопируйте и вставьте URL-адрес из браузера).
5. При необходимости измените любые настройки по умолчанию.

Опция	Описание
#Tests (Количество тестов)	Количество последовательных запусков теста.
Download Success Rate (Коэффициент успешной загрузки)	Процент успешной загрузки для количества запусков теста.
Download Average Throughput (Средняя пропускная способность загрузки)	Требуемая средняя скорость в килобитах в секунду для успешного прохождения теста.
Download Average Delay (Средняя задержка загрузки)	Требуемая средняя задержка соединения загрузки для успешного прохождения теста.
Download Maximum Delay (Максимальная задержка загрузки)	Требование к максимальной задержке соединения загрузки для успешного прохождения теста.

Настройка Multimedia

Опция Multimedia позволяет проверить возможность подключения к мультимедиа, например к видео или аудиофайлу.

1. Щелкните кнопкой мыши на Config (Настроить).
2. Откройте вкладку Multimedia.
3. Нажмите New (Создать) и введите имя теста. Нажмите кнопку OK.
4. Выбрав имя теста, введите URL-адрес, заканчивающийся именем мультимедийного файла (или скопируйте и вставьте URL-адрес из браузера).
5. При необходимости измените любые настройки по умолчанию.

Опция	Описание
#Tests (Количество тестов)	Количество последовательных запусков теста.
Duration (Продолжительность)	Время в миллисекундах для запуска теста.
Timeout (Таймаут)	Время в миллисекундах до прерывания теста.
Success Rate (Степень успешности)	Процент успешных запусков для успешности теста.
Play Average Delay (Средняя задержка воспроизведения)	Средняя задержка связи с хостом в миллисекундах.
Max Delay (Максимальная задержка)	Максимальная задержка связи с хостом в миллисекундах.
Average Throughput (Средняя пропускная способность)	Средняя требуемая скорость в килобитах в секунду для успешного прохождения теста.
Frame Skipped (Пропущено кадров)	Общее количество кадров, пропущенных во время воспроизведения.
Lost Packets (Потерянные пакеты)	Количество потерянных пакетов. Этот метод позволяет извлекать только пакеты потокового мультимедиа, и значение будет равно нулю при использовании протокола HTTP (без потерь). Пакеты могут теряться по ряду причин, например, из-за типа и качества сетевого подключения. Каждый раз, когда воспроизведение останавливается и запускается снова, значение, полученное с помощью этого метода, сбрасывается на ноль. Если воспроизведение приостановлено, значение не сбрасывается. Этот метод позволяет получить достоверную информацию только во время выполнения, когда установлен URL-адрес для воспроизведения.

Bandwidth (Полоса пропускания)	Текущая пропускная способность мультимедийного элемента. Данная опция применима только для мультимедийного потока.

Поддерживаемые форматы мультимедиа:
ASF AIF AIFC AIFF AU
AVI MID MPE MPEG MPG
MPv2 MP2 MP3 M1V SND
WAV
Файлы Windows Media с расширением имени файла .wm
Windows Media Audio (WMA)
Windows Media Video (WMV)

В настоящее время Windows Media Player поддерживает следующие протоколы:

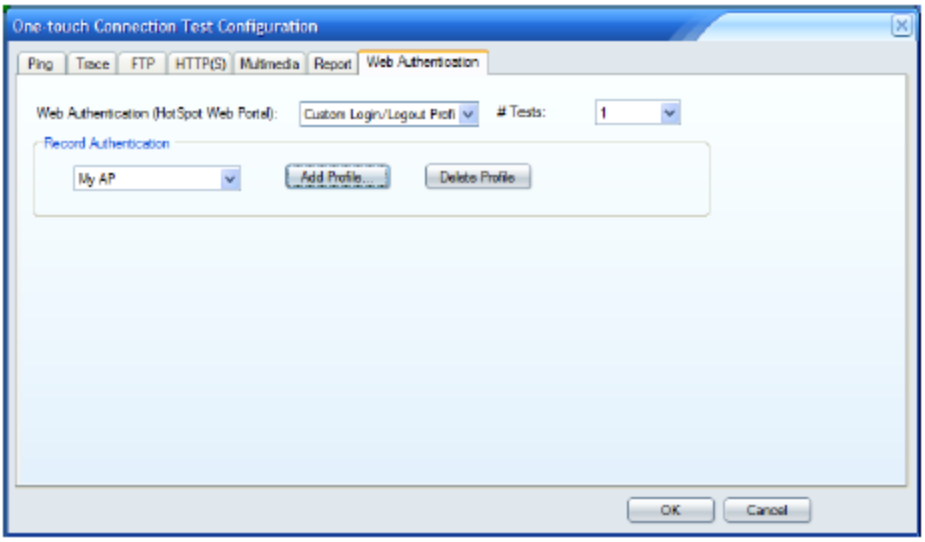
Протокол	Описание
HTTP	Протокол передачи гипертекста. Включает HTTP с быстрым кешированием и многоадресной рассылкой.
RTSP	Протокол потоковой передачи в реальном времени. Включает RTSP с быстрым кешированием.
RTSPU RTSP	Используется с протоколом пользовательских дейтаграмм (UDP). Включает RTSPU с быстрым кешированием.
RTSPT RTSP	Используется с протоколом управления передачей (TCP). Включает RTSPT с быстрым кешированием.
MMS	Протокол Microsoft Media Server.
MMSU	MMS, используемый с UDP.
MMST	MMS, используемый с TCP.
WMPCD	Протокол, используемый проигрывателем Windows Media Player для обеспечения доступа к компакт-дискам.
WMPDVD	Протокол, используемый проигрывателем Windows Media Player для обеспечения доступа к дискам DVD-ROM.

Настройка веб-аутентификации

Инструмент Web Authentication (Веб-аутентификация) позволяет тестировать аутентификацию в случае, когда точка доступа автоматически перенаправляется на веб-сайт, который требует аутентификации, например, входа и выхода.

1. В окне One Touch Connection Tool щелкните кнопкой мыши на Config.
2. Откройте вкладку Web Authentication (Веб-аутентификация).
3. Выберите опции из разворачивающегося списка:
   - None (Нет): Это значение по умолчанию, при котором тест веб-аутентификации не используется.
   - Manual Test (Ручное тестирование): Выбирайте эту опцию, если для аутентификации не требуется ввод пароля, но необходимо ручное вмешательство, например установка метки в поле для принятия условий.
   - Custom Login/Logout Profile (Пользовательский профиль входа/выхода): Выберите эту опцию, чтобы создать профиль для веб-сайта, который имеет защиту с использованием пароля.

4. Если выбран вариант Custom Login/Logout Profile (Пользовательский профиль входа/выхода), необходимо будет создать профиль входа/выхода.



5. Нажмите Add Profile (Добавить профиль). Введите имя профиля и нажмите кнопку OK.
6. Выберите AP/SSID из разворачивающегося списка и нажмите Connect (Подключиться). Будет установлена связь с точкой доступа.

Примечание: Для любой защищенной паролем точки доступа/SSID необходимо настроить профиль в основной конфигурации приложения WiFi Analyzer на вкладке 802.11.

7. Нажмите Next (Далее). Откроется веб-страница.
8. Нажмите Start Record (Начать запись). Войдите на веб-страницу. Нажмите Stop Record (Остановить запись). Нажмите Next (Далее).
9. Нажмите Start Record (Начать запись). Выйдите из веб-страницы. Нажмите Stop Record (Остановить запись). Нажмите Finish (Готово).

Для завершения настройки веб-аутентификации выберите количество запусков этого теста в разворачивающемся списке #Tests.

Запуск теста One Touch Connection Test

После настройки одного или нескольких тестов запустите тестирование. Последовательно можно запустить один или несколько тестов.

1. Откройте вкладку на панели навигации для нужных тестов: Ping/Trace, FTP/HTTP или Multimedia.
2. Отметьте, какие тесты нужно запустить.
3. Нажмите Start (Пуск).

Тесты будут запущены, и окно One Touch Connection заполнится результатами тестирования.

Примечание: Если на компьютере включен брандмауэр, он может заблокировать выполнение одного или нескольких тестов. В этом случае может появиться сообщение о том, что брандмауэр включен. Остановите тест (нажав кнопку Stop) и отключите брандмауэр.

Во время выполнения тестов соответствующая вкладка на панели навигации будет мигать.

4. Для отмены теста нажмите Stop (Остановить).

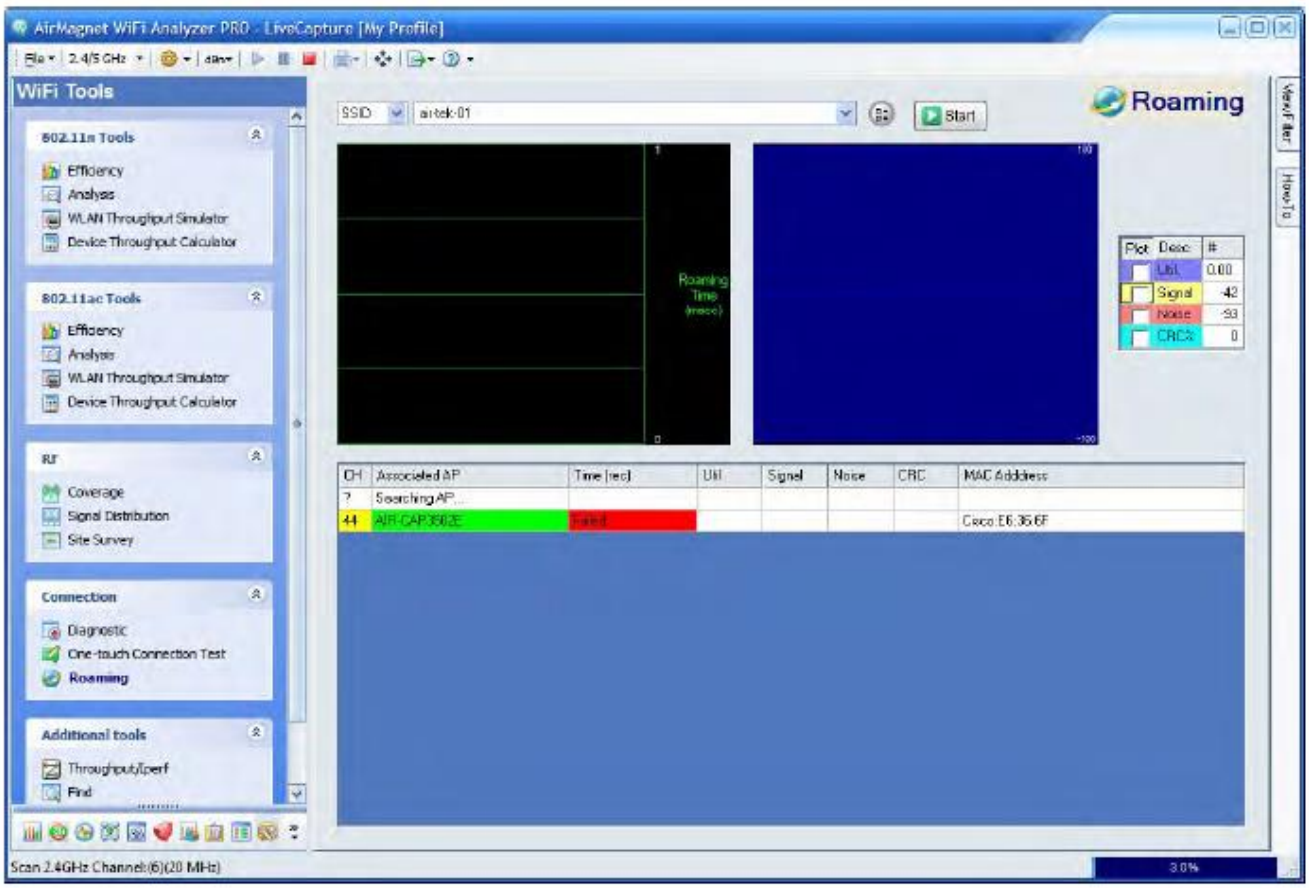
Результаты теста One Touch Connection

По завершении теста результаты появятся в окне One Touch Connection Test. Для просмотра результатов открывайте соответствующие вкладки на панели навигации.
Если в поле Create One Touch Connection Test Report (Создать отчет о тестировании соединения одним нажатием) была поставлена метка, станет доступна кнопка Report (Отчет). Нажмите кнопку Report, чтобы создать отчет.

Результаты тестирования соединения одним нажатием

Инструмент Roaming (Роуминг)

Инструмент Roaming – это еще одна утилита для поиска и устранения неисправностей на сетях VoWLAN. Ключевым компонентом QoS для VoWLAN является способность таких сетей позволять станциям перемещаться между точками доступа без потери вызовов. Если время переключения слишком велико, вероятность того, что вызовы будут прерваны, значительно возрастает. С помощью инструмента Roaming (Роуминг) приложения AirMagnet WiFi Analyzer можно измерять задержку роуминга, то есть промежуток времени между отсоединением станции от одной точки доступа и последующим соединением с другой точкой доступа. На рисунке ниже показан экран инструмента Roaming (Роуминг) приложения AirMagnet WiFi Analyzer. Обратитесь к разделам «Настройка инструмента Roaming (Роуминг)» и «Проведение тестов роуминга».



Настройка инструмента Roaming (Роуминг)

Для измерения возможности подключения в роуминге:

1. На экране инструмента Roaming (Роуминг) щелкните кнопкой мыши на  (Настроить).

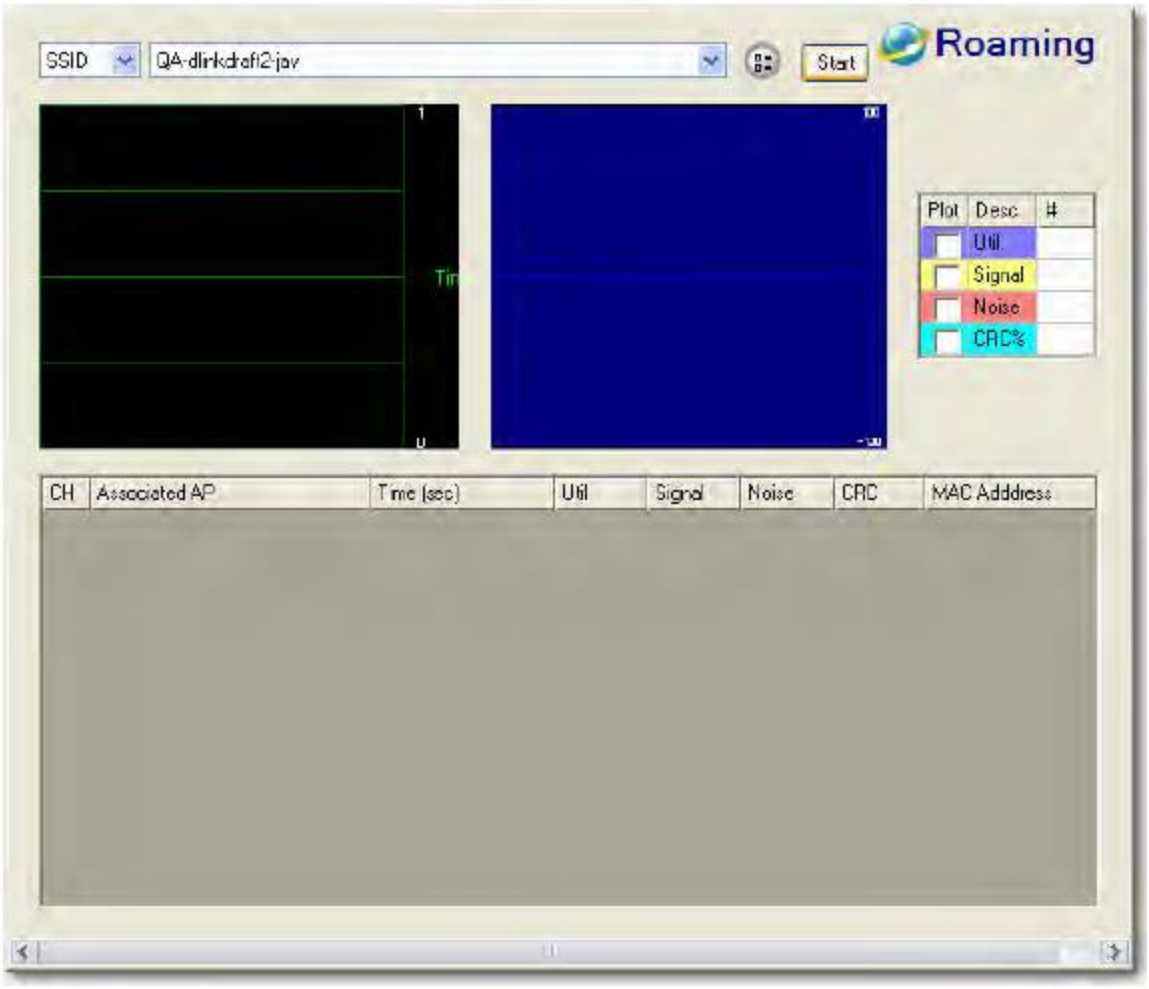
2. В диалоговом окне Roaming Options (Параметры роуминга) сделайте требуемый выбор.
3. Нажмите кнопку OK.

Проведение тестов роуминга

Для проведения теста роуминга:

1. В верхней части экрана инструмента Roaming (Роуминг) выберите SSID или AP, затем выберите конкретную точку доступа или идентификатор SSID в разворачивающемся списке.
2. Нажмите Start.

Данные начнут появляться на экране.



3. Чтобы завершить тест роуминга, нажмите Stop.

Инструмент Roaming (Роуминг) проверяет способность устройства переключаться между двумя точками доступа, а также замеряет время, необходимое для установления связи. Данные на экране позволят обнаружить существующие проблемы. На панели графика справа отображаются данные, поля которых отмечены в разделе справа от этой панели. Можно отметить любое поле или все различные поля данных, чтобы составить диаграмму для любого типа данных, которые вас интересуют.

Дополнительные инструменты

Throughput/Iperf (Пропускная способность/Iperf)

Приложение AirMagnet WiFi Analyzer интегрируется с Iperf - бесплатным программным инструментом с открытым исходным кодом для анализа производительности сети. Такая интеграция позволяет анализировать полосу пропускания и пропускную способность (TCP и UDP), а также джиттер и потерянные/все дейтаграммы из пользовательского интерфейса приложения AirMagnet WiFi Analyzer.

Для использования всех преимуществ интеграции приложения AirMagnet WiFi Analyzer с Iperf необходимо загрузить и установить Iperf версии 1.7.0, которая была протестирована и была подтверждена ее возможность работы с приложением AirMagnet WiFi Analyzer 8.0 и более поздних версий. Обратитесь к разделам «Установка программного обеспечения Iperf» и «Анализ полосы пропускания и пропускной способности».

Установка программного обеспечения Iperf

Интеграция AirMagnet Survey с программным обеспечением Iperf с открытым исходным кодом предоставляет средства записи скорости передачи для выгрузки и загрузки данных во время активного обследования. Хотя по сравнению с активными обследованиями для этого требуется некоторая дополнительная настройка, возможность просмотра информации о скорости выгрузки и загрузки может быть очень важна при анализе среды беспроводной сети.

Во время обследования Iperf портативный компьютер, который используется для проведения обследования, передает пользовательские пакеты данных Iperf на настроенный пользователем сервер Iperf. Ответы сервера позволяют записывать скорость загрузки станции из текущего местоположения.
Для проведения активного обследования Iperf необходимо загрузить и разархивировать на отдельном устройстве программное обеспечение сервера Iperf. Программное обеспечение Iperf можно найти в сети Интернет по запросу «iperf 1.7». Интеграция Iperf предназначена для работы с Iperf Server версии 1.7.0.

Примечание: Для хранения файлов мы рекомендуем создать папку Iperf в корневом каталоге (то есть C:\Iperf).

Запуск сервера Iperf

После загрузки и распаковки программного обеспечения сервера Iperf перед началом обследования Iperf необходимо запустить приложение.

1. Чтобы открыть диалоговое окно Run (Выполнить), щелкните кнопкой мыши на Start > Run (Пуск > Выполнить).
2. Чтобы открыть интерфейс командной строки Windows, введите cmd и нажмите кнопку OK.
3. Перейдите в папку Iperf (например, C:\Iperf), введите «Iperf -s» и нажмите Enter. Появится сообщение с описанием TCP-порта, используемого сервером.

Примечание: В команде запуска сервера Iperf параметр -s означает «сервер», а часть «-p 5001» указывает серверу прослушивать порт 5001. По умолчанию приложение AirMagnet Survey использует порт 5001 в качестве порта передачи во время активного обследования Iperf. Если порт сервера Iperf изменен, также необходимо изменить порт, используемый приложением Survey.

Как только появляется сообщение о состоянии сервера Iperf, система активно прослушивает сообщения передачи Iperf. Теперь система готова к проведению активного обследования Iperf.

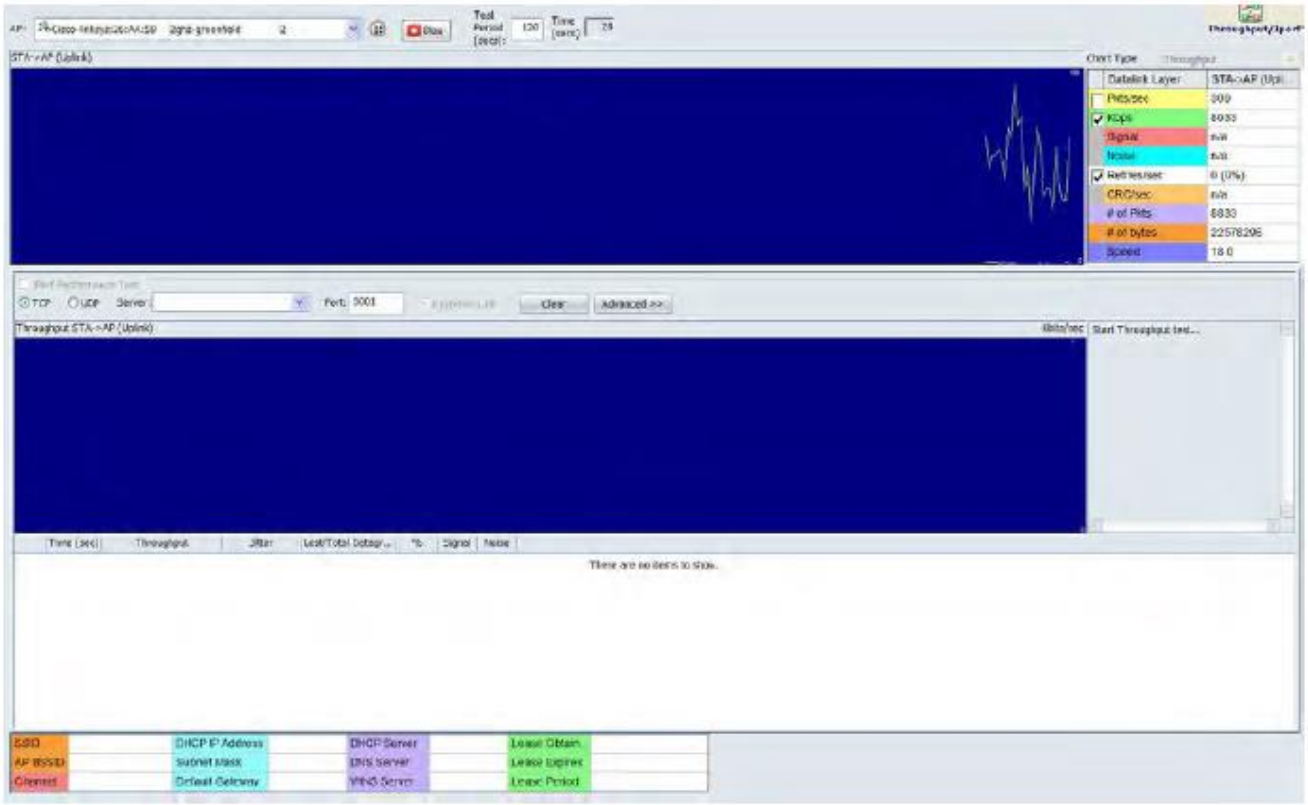
Анализ полосы пропускания и пропускной способности сети с помощью Iperf

Для анализа полосы пропускания и пропускной способности сети с помощью Iperf:

1. На экране WiFi Tools (Инструменты WiFi) нажмите Throughput/Iperf (Пропускная способность/Iperf). Появится экран Throughput/Iperf.
2. Выберите точку доступа.
3. Укажите продолжительность периода тестирования (Test Period), например, 120.
4. Выберите тип диаграммы (Chart Type), например, PHY Data Rate (Скорость передачи данных физического уровня).

5. Обязательно поставьте метку в поле Iperf Performance Test.
6. Выберите TCP или UDP и укажите сервер (Server) и порт (Port).
7. Поставьте метку в поле Up/Downlink.
8. Нажмите 

. Данные начинают появляться на экране, как показано в примере ниже.



Примечания:

- Тест завершается автоматически по истечении указанного периода тестирования. Кроме того, тест можно остановить в любой момент, нажав кнопку 

.
- В приведенном выше примере показано, что пропускная способность сети измеряется скоростью передачи данных физического уровня (PHY Data Rate). Скорости передачи данных физического уровня для нисходящего и восходящего каналов составляют 2072 Кбит/с и 696 Кбит/с (крайняя правая полоса каждой гистограммы) соответственно. Для нисходящего канала 100% пропускной способности (2072 Кбит/с) используют данные со скоростью 27 Мбит/с. Для восходящего канала 100% пропускной способности (696 Кбит/с) использует скорость передачи данных 108 Мбит/с.

Экран Throughput/Iperf (Пропускная способность/Iperf) содержит два отдельных инструмента для проведения тестов производительности сети. Верхняя половина – это «старый» инструмент AirMagnet WiFi Analyzer Performance, доступный в приложении AirMagnet WiFi Analyzer 7.x или более ранней версии; нижняя половина – это инструмент Iperf, который стал доступен только с этим приложением AirMagnet WiFi Analyzer 9.0 и более поздними версиями приложения AirMagnet WiFi Analyzer PRO.
При запуске теста производительности Iperf с использованием UDP и включенной (отмеченной) опцией Up/Down Link, не прерывайте тест, нажимая кнопку Stop. Это может привести к закрытию сервера Iperf.

Расширенные свойства Iperf

На приведенном ниже экране показаны расширенные свойства Iperf.

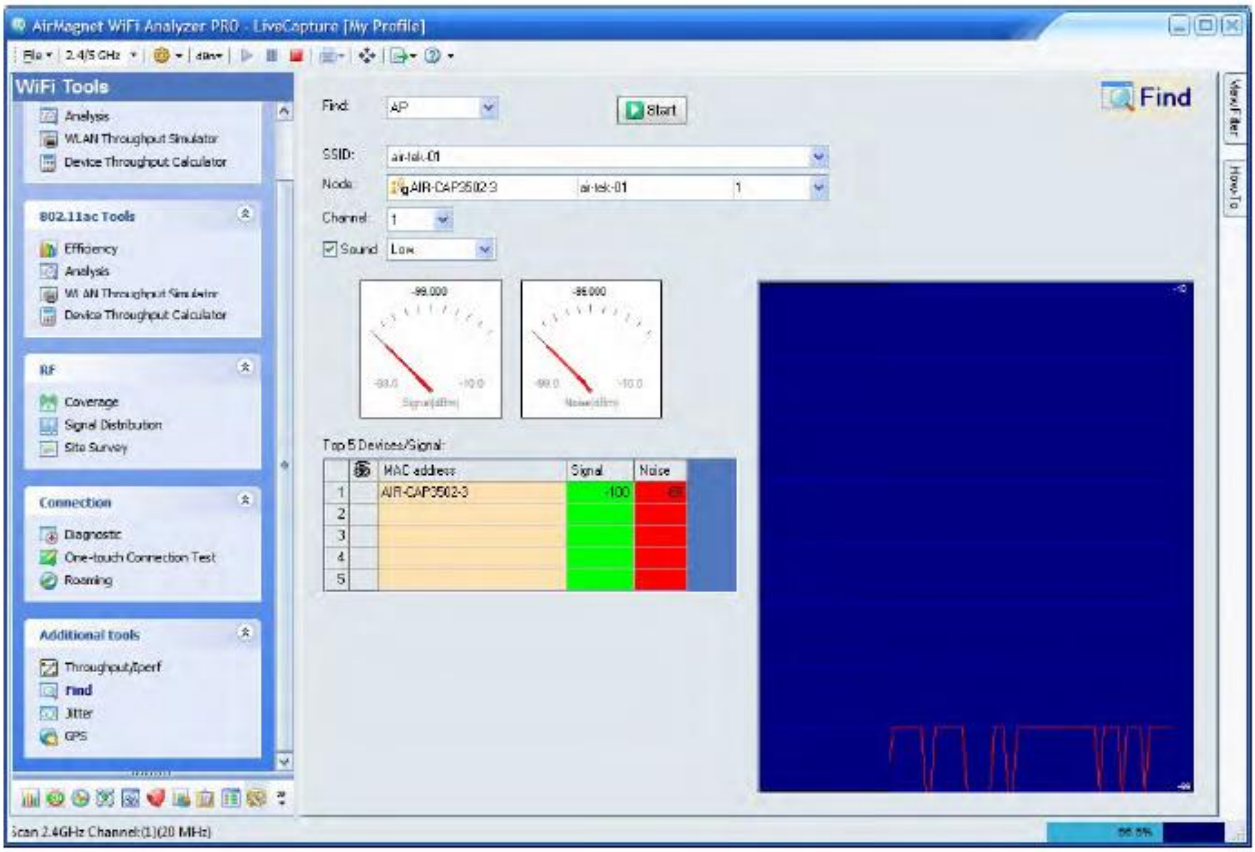
В таблице ниже описаны расширенные свойства инструмента Iperf.

Свойство	Описание
Compatibility (Совместимость)	В случае выбора этот параметр обеспечивает обратную совместимость с более старой версией Iperf.
Client Port (Порт клиента)	Порт, через который сервер Iperf соединяется с клиентом. По умолчанию применяется порт, используемый для подключения к серверу Iperf от клиента.
TCP Window Size (Размер окна TCP)	Устанавливает указанное значение в качестве размера буфера сокета. Для TCP это устанавливает размер окна TCP. Для UDP это просто буфер, в который принимаются дейтаграммы, что ограничивает максимальный размер принимаемой дейтаграммы.
Buffer Length (Длина буфера)	Длина буфера для чтения или записи. При работе Iperf записывает массив размером len байтов несколько раз. По умолчанию это 8 КБ для TCP и 1470 байт для UDP. Примечание для UDP: это размер дейтаграммы, который необходимо уменьшить при использовании IPv6-адресации до 1450 или меньшего значения, чтобы избежать фрагментации.
Max Segment Size (Максимальный размер сегмента)	Позволяет установить максимальный размер сегмента TCP (MSS). Обычно TMSS – это байты MTU-40 для заголовка TCP/IP. Для Ethernet MSS составляет 1460 байт (MTU 1500 байт).
Parallel Streams (Параллельные потоки)	Количество одновременных подключений к серверу. По умолчанию 1. Примечание: Эта функция требует поддержки потоков как на клиенте, так и на сервере.
Bandwidth UDP (Полоса пропускания UDP)	Пропускная способность UDP для отправки в бит/сек. По умолчанию 1 Мбит/сек.
Bind to Host (Привязать к хосту)	Один из адресов этого хоста (компьютера). Для клиента устанавливает исходящий интерфейс; для сервера устанавливает входящий интерфейс. Это полезно только на многосетевых хостах, у которых есть несколько сетевых интерфейсов. Для Iperf в режиме сервера UDP этот параметр также используется для связывания и присоединения к группе многоадресной рассылки, и в этом случае следует использовать адреса в диапазоне от 114.0.0.0 до 239.255.255.255.
Representative File (Репрезентативный файл)	Нажмите кнопку, чтобы выбрать репрезентативный поток для измерения пропускной способности.
Type of Service (Тип обслуживания)	Выберите тип обслуживания для исходящих пакетов из следующих вариантов: • Low Cost (Низкая стоимость) • Low Penalty (Низкий штраф) • Reliability (Надежность) • Throughput (Пропускная способность)
TTL	Время жизни исходящих многоадресных пакетов. По сути, это количество проходов маршрутизаторов, которое также используется для определения границ. По умолчанию - 1, локальное соединение.

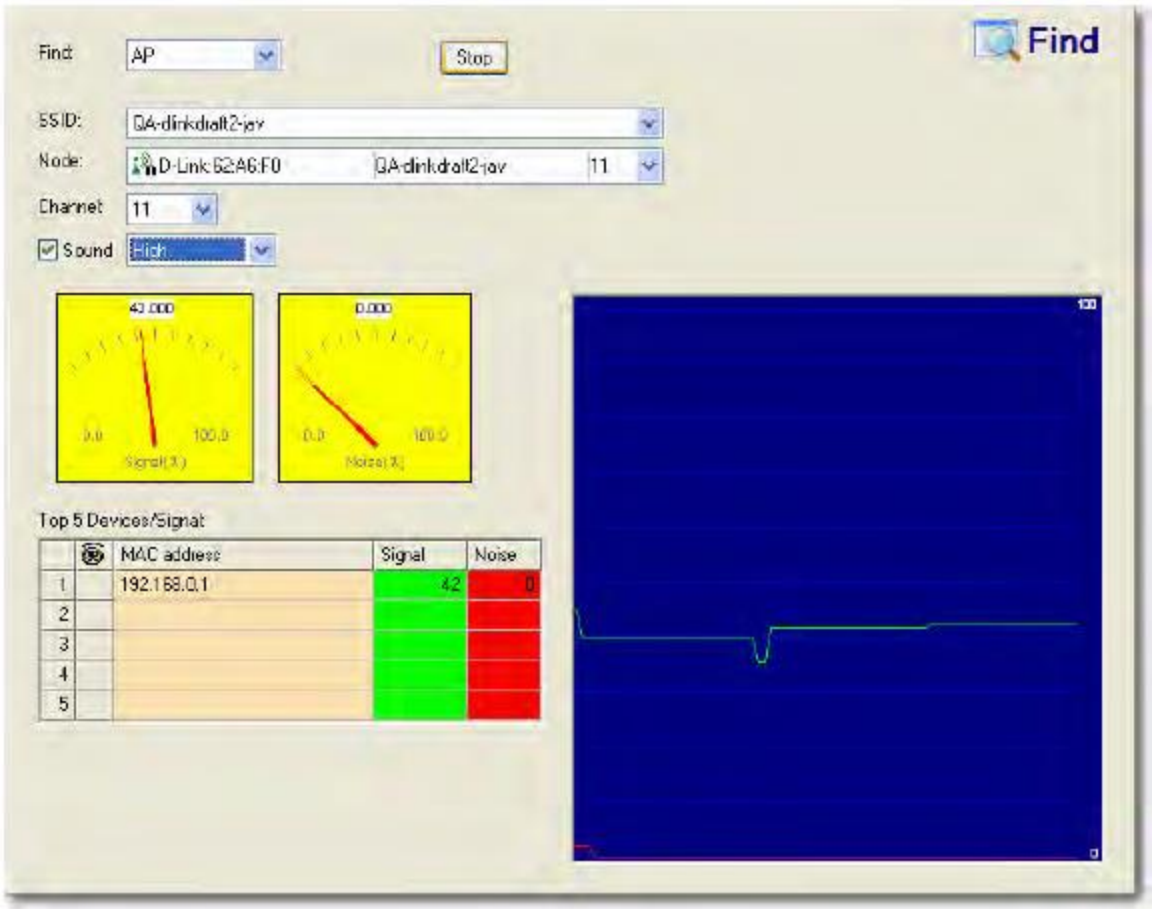
TCP No Delay (TCP без задержки)	Если в этом поле стоит метка, устанавливается параметр TCP без задержки, и отключается алгоритм Наггла. Обычно отключается только для интерактивных приложений, таких как telnet.
Output Format (Формат вывода)	Щелкните кнопкой мыши на направленной вниз стрелке и выберите в разворачивающемся списке формат, в котором должны распечатываться значения пропускной способности. Поддерживаемые форматы: • Adaptive Bits (Адаптивные биты) • Adaptive Bytes (Адаптивные байты) • Bits (Биты) • Bytes (Байт) • Kbits (Кбит) • Kbytes (Кбайт) • Mbits (Мбит) • Mbytes (Мбайт)
Print MSS (Печатать MSS)	Если выбран этот параметр, включается печать сообщаемого размера TCP mSS (с помощью параметра TCP_MAXSEG) и наблюдаемых размеров чтения, которые часто коррелируют с MSS. MSS обычно представляет собой MTU - 40 байт для заголовка TCP/IP. Часто сообщается о немного меньшем MSS из-за дополнительного пространства заголовка из параметров IP. Также печатается тип интерфейса, соответствующий MYU (Ethernet, FDDI и т.д.). Данная опция не реализована во многих операционных системах, но размеры чтения все еще могут указывать MSS.

Инструмент Find (Найти)

Приложение AirMagnet WiFi Analyzer не только может обнаруживать присутствие любых беспроводных устройств (включая неавторизованные точки доступа и станции), но также способно помочь определить физическое местоположение любых обнаруженных устройств. Это легко сделать с помощью инструмента Find (Найти) приложения AirMagnet WiFi Analyzer. На рисунке ниже показан экран инструмента Find (Найти). Также обратитесь к разделу «Обнаружение местоположения неавторизованных устройств».



Обнаружение местоположения неавторизованных устройств



Для поиска неавторизованного устройства:

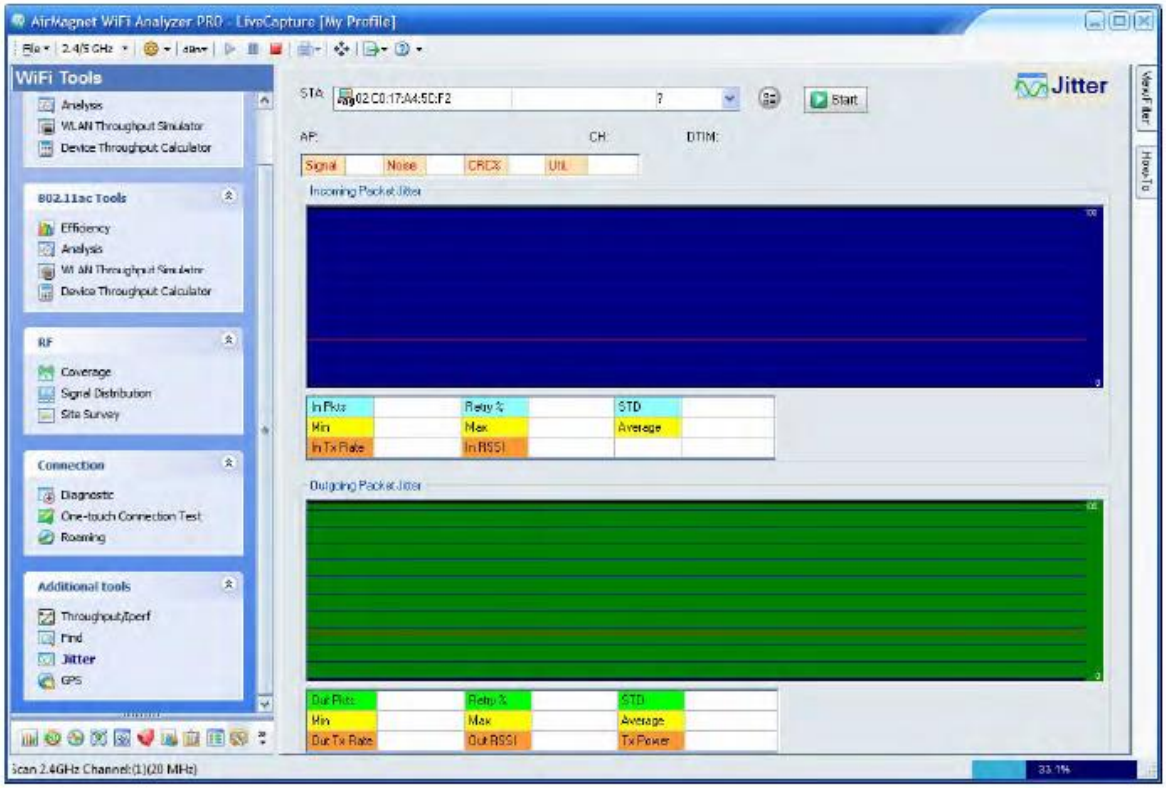
1. На экране AirWISE найдите сигналы тревоги в разделе Rogue AP and Station (Неавторизованная точка доступа и станция).
2. Идентифицируйте неавторизованное устройство (точку доступа или станцию) и запишите имя его производителя (а после него – три первые цифры его MAC-адреса) и SSID.
3. На экране инструмента Find (Найти) выберите AP (Точка доступа) или STA (Станция).

Примечание: Должно соответствовать типу устройства, которое выбрано на экране AirWISE в шаге 2.

4. Выберите SSID записанного вами неавторизованного устройства.
5. Выберите узел, если возможно.
6. Выберите канал, на котором работает неавторизованное устройство, если это возможно.
7. Нажмите Start. MAC-адреса пяти ведущих точек доступа или станций с тем же SSID появятся в таблице, причем точка доступа с самым сильным сигналом будет возглавлять список.
8. На панели Top 5 Devices/Signal (Пять ведущих устройств/сигналов) щелкните кнопкой мыши на поле рядом с устройством, которое хотите найти.
9. Включите звук и установите высокий уровень громкости (High). Это упростит поиск неавторизованного устройства.
10. Смотрите на измеритель сигнала и идите в том направлении, где сигнал по мере движения становится сильнее, пока не обнаружите устройство физически.
11. Нажмите Stop, чтобы завершить данную операцию.

Инструмент Jitter (Джиттер)

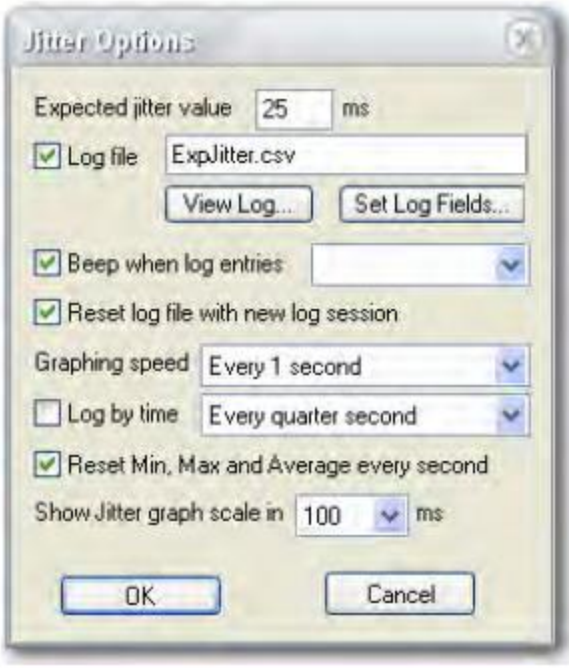
Под джиттером понимается нежелательное изменение частоты или фазы цифрового или аналогового сигнала. Телефоны и системы VoWLAN спроектированы с учетом определенного уровня джиттера в сети. Однако если значение джиттера становится слишком высоким, может пострадать качество вызовов или сетевых подключений. Инструмент Jitter приложения AirMagnet WiFi Analyzer позволяет администраторам сети легко проверять значение джиттера в сети VoWLAN, чтобы гарантировать требуемое качество обслуживания (QoS) для голосового трафика. На рисунке ниже показан экран инструмента Jitter приложения AirMagnet WiFi Analyzer. Обратитесь к разделу «Настройка инструмента Jitter (Джиттер)» и «Проведение тестов джиттера».



Настройка инструмента Jitter (Джиттер)

Чтобы инструмент Jitter (Джиттер) мог работать так, как вам нужно, его необходимо настроить.

Для настройки параметров инструмента Jitter:



1. На экране WiFi Tools > Jitter (Инструменты WiFi > Джиттер) щелкните кнопкой мыши на  (Настроить).
2. Сделайте желаемый выбор и нажмите кнопку OK.

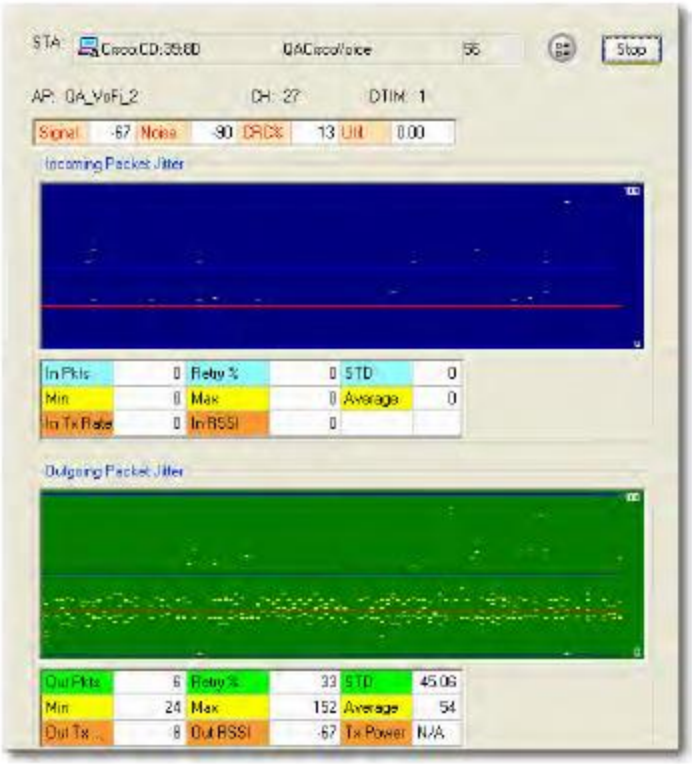
Проведение тестов джиттера

Для измерения джиттера радиочастотного сигнала в сети:

1. В верхней части экрана инструмента Jitter (Джиттер) щелкните кнопкой мыши на направленной вниз стрелке и выберите интересующую вас станцию из разворачивающегося списка.

2. Нажмите 

. Данные о джиттере начнут появляться на экране, как показано ниже.



3. Для завершения теста нажмите 

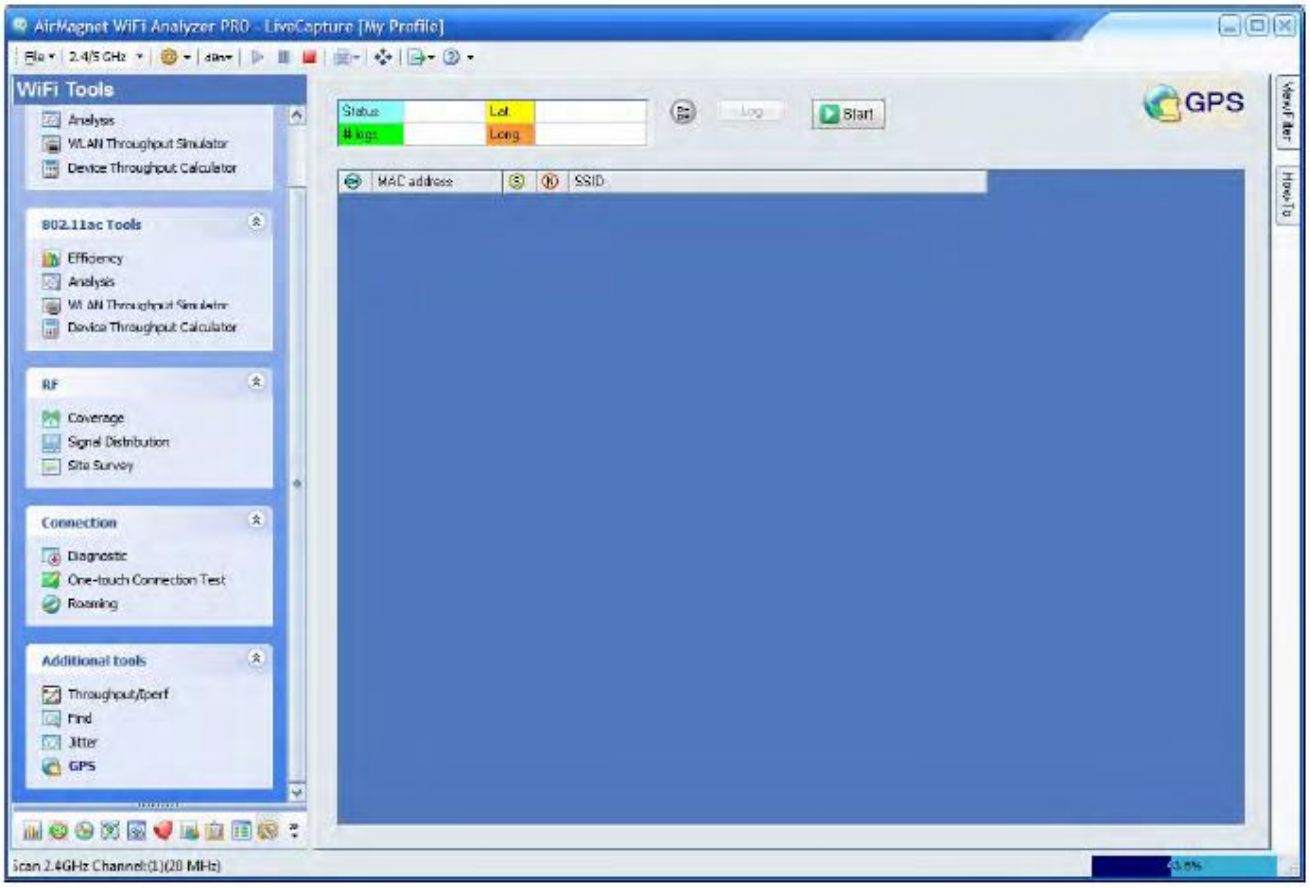
. Отображаемая на экране инструмента Jitter информация описывается в таблице ниже.

Параметр	Описание
AP (Точка доступа)	Точка доступа, с которой связана станция. Определяется автоматически.
CH (Канал)	Канал, на котором работает точка доступа. Определяется автоматически.
Util (Использование)	Коэффициент использования канала.
Noise (Шум)	Уровень шума в дБм.
CRC%	Частота ошибок CRC.
DTIM	Конфигурация DTIM на точке доступа.
In Pkts (Входящие пакеты)	Входящие пакеты от точки доступа.
Retry%	Частота повторных попыток.
STD	Стандартное квадратическое отклонение.
Min.	Минимальное значение джиттера.
Max.	Максимальное значение джиттера.
Average	Среднее значение джиттера.
Out Pkts (Исходящие пакеты)	Исходящие пакеты к точке доступа.
Верхний график	Распределение джиттера входящих пакетов от 0 до 100 мс.
Нижний график	Распределение джиттера исходящих пакетов от 0 до 100 мс.
Красная горизонтальная линия	Ожидаемое значение джиттера.

Инструмент GPS

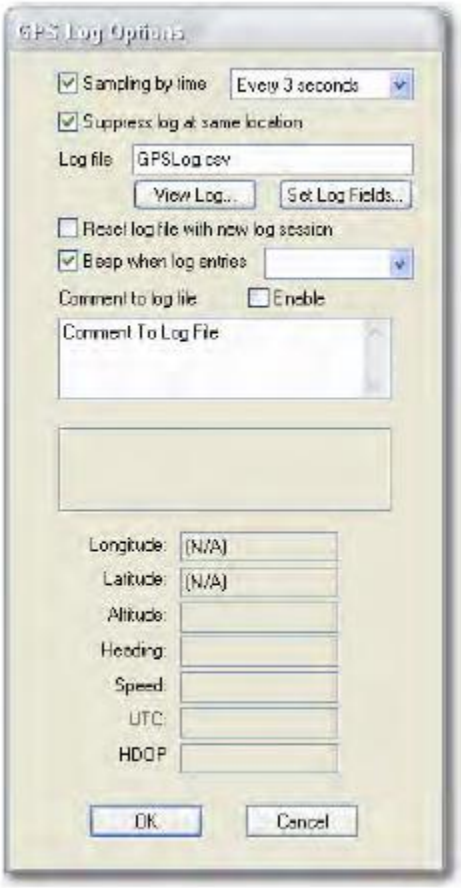
Инструмент GPS позволяет найти точное местоположение устройства, обнаруженного приложением AirMagnet WiFi Analyzer в сети. На рисунке ниже показан экран инструмента GPS приложения AirMagnet WiFi Analyzer. Обратитесь к разделам «Настройка параметров GPS», «Настройка опций GPS» и «Использование инструмента GPS».

Примечание: Перед использованием инструмента GPS необходимо выполнить настройку конфигурации GPS на экране AirMagnet Configuration (Конфигурация AirMagnet) (File > Configure > Profile (Файл > Настроить > Профиль)) и иметь подключенное к своему портативному компьютеру устройство GPS.



Настройка опций GPS

Для правильного использования приложения AirMagnet WiFi Analyzer с GPS необходимо настроить инструмент GPS.



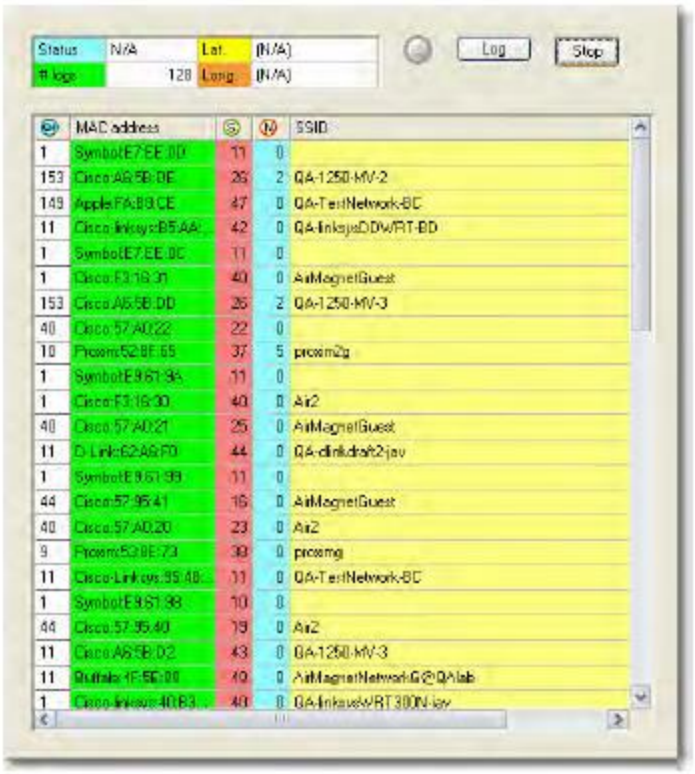
Для настройки инструмента GPS:

1. На экране GPS щелкните кнопкой мыши на  (Опции GPS).
2. Сделайте желаемый выбор в диалоговом окне.
3. Нажмите кнопку OK.

Использование инструмента GPS

Для сбора данных GPS:

1. На экране инструмента GPS нажмите Start. Данные начнут появляться на экране. Смотрите пример ниже.



2. Для завершения операции нажмите Stop.

Управление файлами данных

Об управлении файлами данных

В этом разделе описывается, как управлять файлами журнала данных радиочастотного сигнала, которые захватываются с помощью приложения AirMagnet WiFi Analyzer. AirMagnet не только захватывает и отображает данные беспроводной сети в режиме реального времени, но также позволяет сохранять, распечатывать и экспортировать эти файлы данных для архивирования, совместного использования или дальнейшего анализа.

- Сохранение захваченных радиочастотных данных
- Открытие файлов данных
- Предварительный просмотр данных перед печатью
- Просмотр недавно открытых файлов
- Экспортирование данных
- Экспортирование данных в AirMagnet Reporter

Сохранение захваченных данных

Чтобы развернуть структуру политик на экране управления политиками AirMagnet (AirMagnet Policy Management):

1. Выберите группу политик, например, Security (Безопасность).
2. Выберите категорию политик в этой группе политик, например, User Authentication and Encryption (Аутентификация пользователя и шифрование).
3. Выберите подкатегорию выбранной категории политик, например, WPA-802.1x и TKIP.
4. Выделите конкретный сигнал тревоги в подкатегории политик, например, 802.1x Rekey Timeout Too Long (Слишком большой таймаут смены ключей 802.1x).

Подробное описание политик AirMagnet WLAN приводится в «Справочном руководстве по политикам беспроводной локальной сети AirMagnet», которое находится на компакт-диске с программным обеспечением.

Форматы файлов, поддерживаемые AirMagnet

Приложение AirMagnet WiFi Analyzer поддерживает следующие форматы файлов:

- .amc - собственный формат файлов AirMagnet, который позволяет воспроизводить сохраненные данные, как если бы воспроизводилось видео. Это позволяет повторно просматривать данные в том виде, в котором они были захвачены.
- .ecp - формат файлов Ethereal.
- .cap - формат файлов Sniffer.
- .amm - собственный формат файлов AirMagnet, используемый для поддержки записи на диск и мультиадаптера. Сохранение в этом формате возможно только при включении одной из этих функций.
- .pcap - файлы, сохраненные с опцией 802.11+.

Сохранение нового файла

Для сохранения данных:

1. На любом экране приложения AirMagnet WiFi Analyzer нажмите File > Save (Файл > Сохранить). Откроется диалоговое окно Save As (Сохранить как).

2. Выберите путь к файлу, введите имя файла и выберите формат файла.
3. Нажмите Save (Сохранить).

По умолчанию приложение AirMagnet WiFi Analyzer автоматически сохраняет все файлы трассировки (.amc) в C:\\Program Files\AirMagnet Inc\AirMagnet Wi-Fi Analyzer на вашем компьютере, используя в качестве имени файла дату и время его сохранения. Однако можно использовать другой каталог и/или имя файла, изменив значения по умолчанию. Также можно выбрать другой формат файла.

Сохранение существующего файла под другим именем или в другом формате

После просмотра существующего файла (смотрите следующий раздел) его можно сохранить под другим именем или в другом формате.

Для переименования файла:

1. Щелкните кнопкой мыши на File > Save As (Файл > Сохранить как). Откроется диалоговое окно Save As (Сохранить как).
2. Выберите путь к файлу, переименуйте файл или выберите другой формат файла.
3. Нажмите Save (Сохранить).

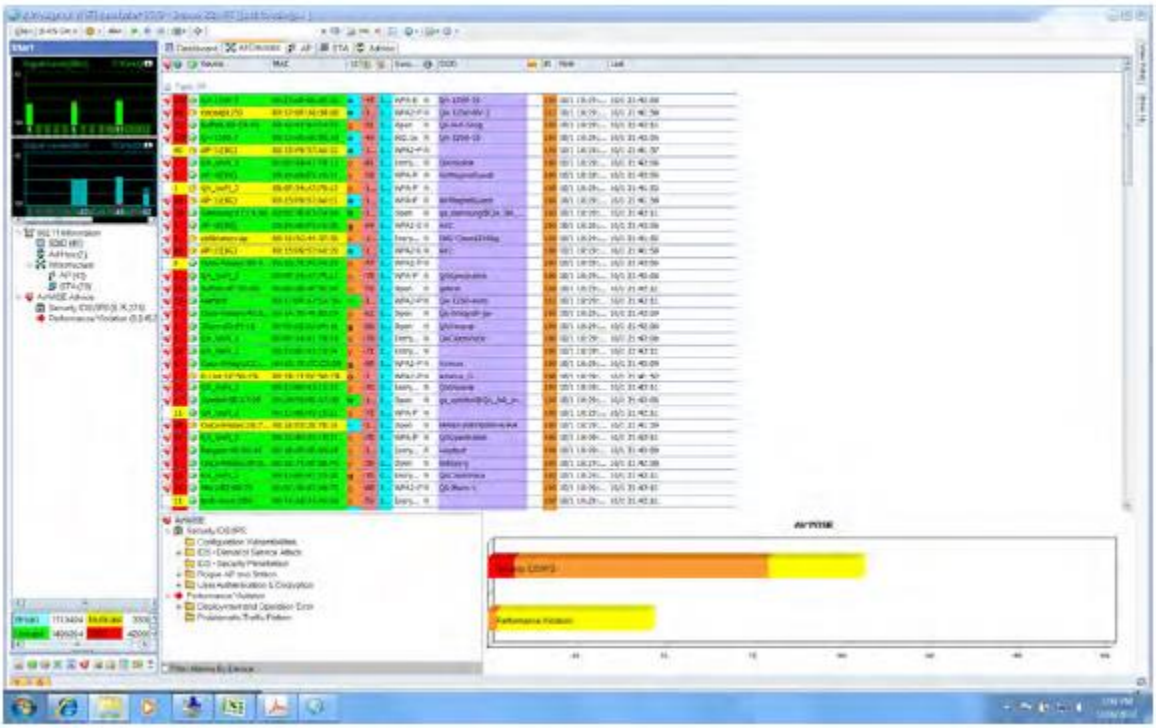
Открытие сохраненного файла

Файлы, сохраненные в любом из поддерживаемых AirMagnet форматов, можно открыть в приложении AirMagnet WiFi Analyzer. Это позволяет повторно просматривать радиочастотные данные, ранее захваченные в вашей беспроводной сети.

Файлы трассировки приложения AirMagnet WiFi Analyzer (.amc) можно открыть двумя способами, в зависимости от того, выбран ли при открытии файла параметр Load Statistics on Open Capture File (Загружать статистику при открытии файла захвата) (File > Configure… > General (Файл > Настроить... > Общие). Если опция НЕ используется, приложение AirMagnet WiFi Analyzer будет воспроизводить только объем данных, сохраненных в буфере, размер которого был установлен во время сохранения файла трассировки. В этом случае в строке заголовка открываемого файла трассировки по мере выполнения отображается ход операции загрузки файла в процентах (%). Однако если используется опция Load Statistics on Open Capture File (Загружать статистику при открытии файла захвата), приложение AirMagnet WiFi Analyzer в дополнение к данным в буфере загрузит все сигналы тревоги (вместе с некоторыми другими важными данными), содержащиеся в файле трассировки. В этом случае файл загружается намного быстрее, поскольку основное внимание уделяется отображению всех данных на экране, а не их воспроизведению в том виде, в каком они были захвачены. По этой причине в строке заголовка открытого файла трассировки отображается только имя файла.

Чтобы открыть файл захвата:

1. Щелкните кнопкой мыши на File > Open… (Файл > Открыть). Откроется экран Open (Открыть).
2. Выберите файл и нажмите Open (Открыть). Данные файла начнут появляться на экране.



3. Подождите, пока значение в верхней части экрана не достигнет 100% (то есть данные будут полностью загружены).
4. Во время и после открытия файла функция захвата в реальном времени приостанавливает свою работу. Чтобы возобновить захват в реальном времени, щелкните кнопкой мыши на  .

Примечание: На рисунке выше показан файл трассировки, открываемый без использования параметра Load Statistics on Open Capture File (Загружать статистику при открытии файла захвата). Открытие файла трассировки таким способом занимает больше времени, особенно если это большой файл. Однако процесс загрузки файла всегда можно ускорить, нажав клавишу F4. В качестве альтернативы, если при открытии файла используется функция Load Statistics on Open Capture File (Загружать статистику при открытии файла захвата), файл загружается мгновенно, и вы сможете увидеть гораздо больше данных, как показано на следующем рисунке.

Просмотр недавно открытых файлов захвата

Приложение AirMagnet WiFi Analyzer отслеживает четыре последних открытых файла в списке последних файлов (Recent Files) в меню File (Файл). Это облегчает доступ к этим файлам.

Для получения доступа к недавно открытому файлу:

1. Щелкните кнопкой мыши на File > Recent Files (Файл > Последние файлы). На экране появляется всплывающий список, в котором отображаются четыре последних открытых файла.

2. В разворачивающемся списке выберите файл, который нужно открыть.

Экспортирование файлов базы данных

По мере сканирования и анализа получаемых пакетов приложение AirMagnet WiFi Analyzer сохраняет в своей внутренней базе данных полную информацию об устройстве беспроводной локальной сети, связанную статистику уровня 1 и уровня 2, а также сгенерированные сигналы тревоги. Содержимое базы данных можно экспортировать в виде набора файлов с разделенными запятыми значениями (.csv), которые затем можно выгрузить на главный компьютер в качестве источников для электронных таблиц Excel или других приложений баз данных.

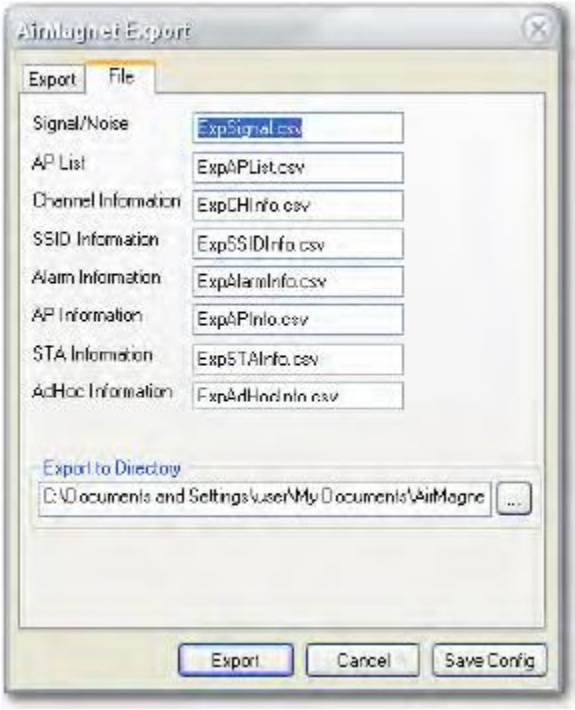
Для экспортирования файлов базы данных:

1. Щелкните кнопкой мыши на  (Импортировать/Экспортировать) и выберите Export… (Экспортировать). Откроется экран Export (Экспортировать).

2. Замените имя сеанса (Session Name) уникальным именем площадки, на которой собираются данные.

Примечание: Каждая операция экспортирования данных называется сеансом. Указание имен сеансов поможет в дальнейшем идентифицировать данные, экспортированные в разное время или в разных случаях.

3. Сделайте желаемый выбор и нажмите Save Config (Сохранить конфигурацию).
4. Откройте вкладку File (Файл). Откроется другой экран, на котором можно изменять имена файлов.

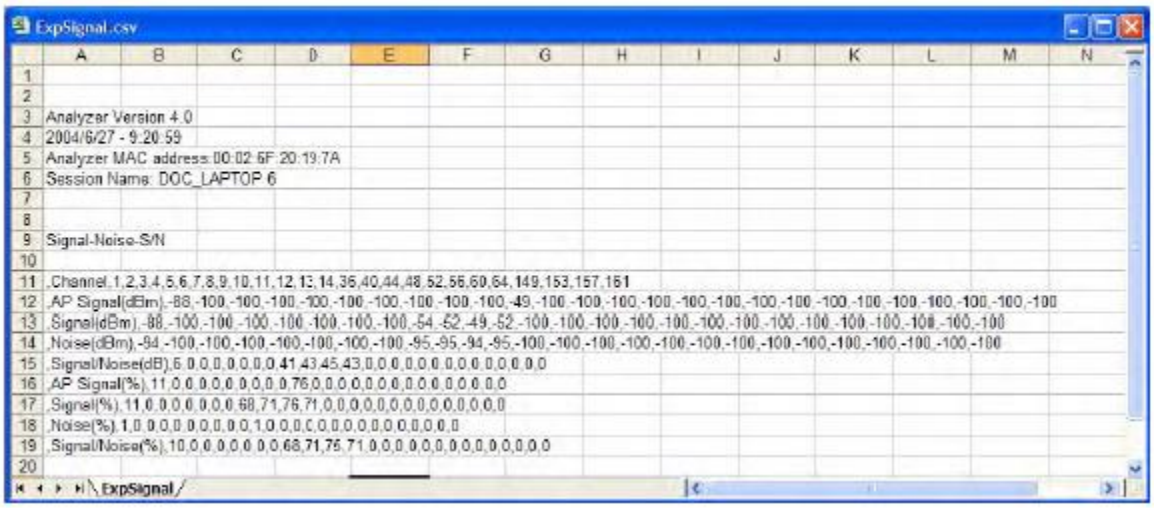


5. При желании переименуйте файлы.
6. Укажите путь к файлу.

7. Нажмите Export (Экспортировать).

Примечание: Расширение файла изменить невозможно.

Файлы .csv можно открывать в приложении Microsoft Excel. На приведенном ниже рисунке показан образец файла .csv.



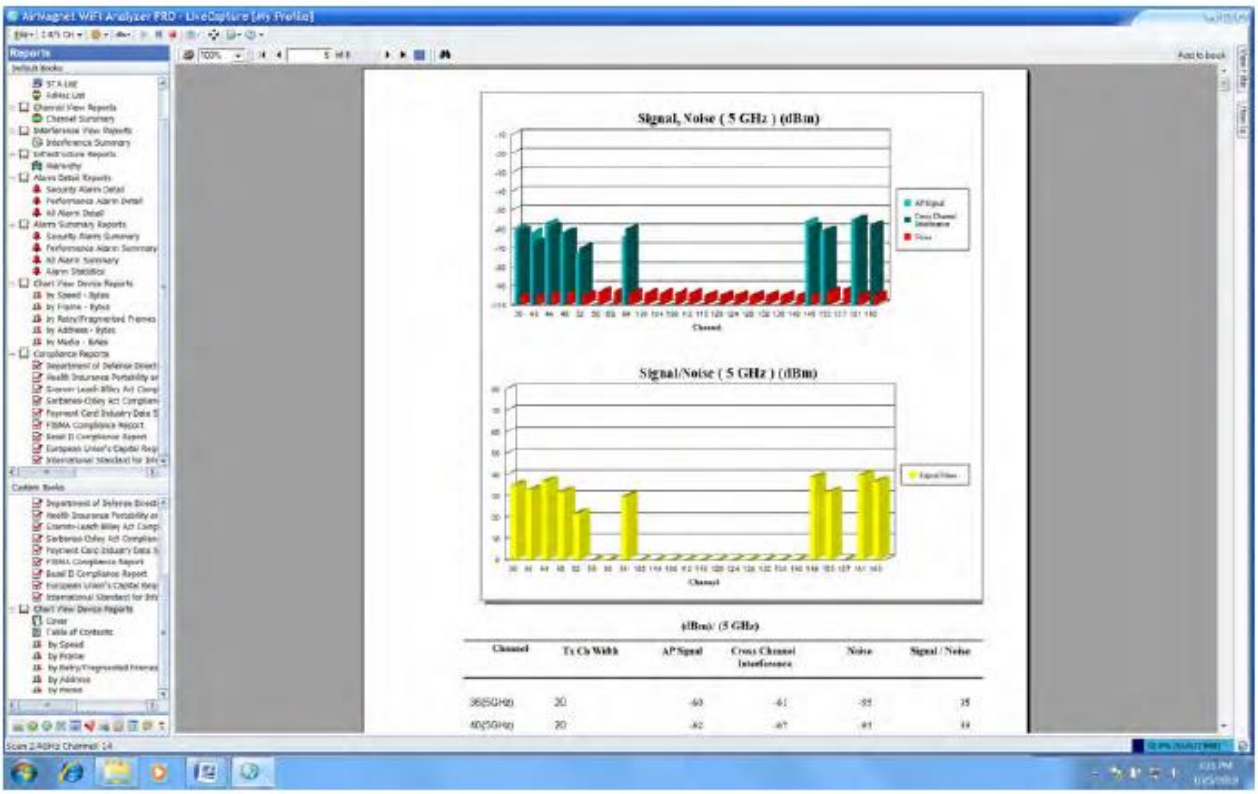
Экран Reports (Отчеты)

Об экране Reports (Отчеты)

Приложение AirMagnet WiFi Analyzer автоматически преобразует захваченные на вашей сети данные в различные отчеты о сетевых данных. Экран Reports (Отчеты) не только позволяет просматривать отчеты о сетевых данных, но также предоставляет инструменты, необходимые для создания пользовательских книг отчетов, представляющих собой коллекции выбранных пользователем отчетов. Это удобный способ организации, совместного использования и архивирования данных, которые собираются в вашей сети.

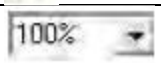
Для перехода к экрану Reports (Отчеты) просто щелкните кнопкой мыши на 

на панели навигации. Экран Reports (Отчеты) приложения AirMagnet WiFi Analyzer показан на рисунке ниже.



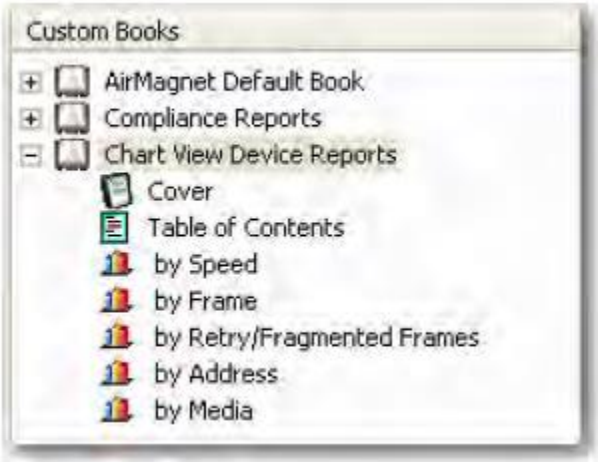
Меню экрана Reports (Отчеты) и доступные инструменты

В следующей таблице описаны меню и инструменты на экране Reports (Отчеты):

Иконка	Название инструмента	Описание
	Печать	Позволяет распечатать текущий открытый отчет.
	Масштаб экрана просмотра	Позволяет установить или изменить масштаб просмотра отчета на экране.
	На первую страницу (отчета)	Позволяет перейти на первую страницу.
	На предыдущую страницу	Позволяет перейти на предыдущую страницу.
	Текущая страница из общего количества страниц	Указывает текущую страницу, а также общее количество страниц отчета.
	На следующую страницу	Позволяет перейти на следующую страницу.
	К последней странице	Позволяет перейти к последней странице.
	Остановить загрузку	Останавливает загрузку выбранного отчета. Примечание: Этот инструмент используется для отмены попытки открытия отчета.
	Текстовый поиск	Позволяет открыть диалоговое окно Search (Найти), в котором можно ввести текст для поиска в текущем открытом отчете.
	Добавить отчет в книгу	Позволяет добавить текущий открытый отчет в (настраиваемую пользователем) книгу отчетов.

Custom Books (Пользовательские книги)

Этот раздел находится в нижнем левом углу экрана Reports (Отчеты). Здесь отображаются все созданные пользователем книги отчетов. Также здесь предоставлены инструменты для создания пользовательских книг отчетов и управления ими.



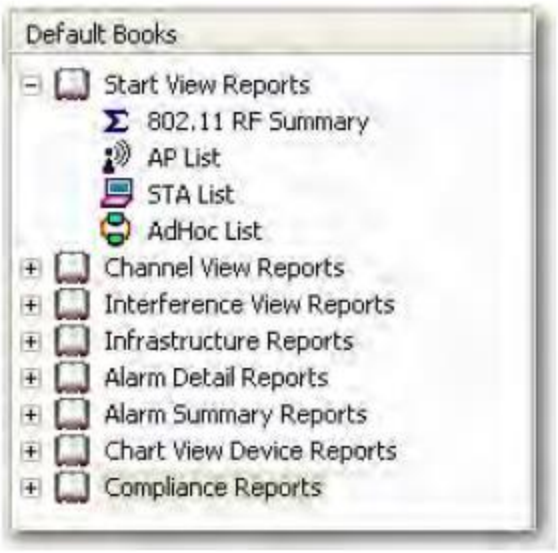
В этой части экрана Reports (Отчеты) можно выполнять следующие задачи:

- Создание книги отчетов
- Добавление отчетов в книгу
- Изменение свойств книги
- Изменение содержания отчета
- Удаление отчета или книги отчетов
- Изменение свойств книги

- Изменение содержания книги

Default Books (Книги по умолчанию)

Этот раздел расположен в верхнем левом углу экрана Reports (Отчеты). В нем перечислены все отчеты, автоматически созданные приложением AirMagnet WiFi Analyzer. Отчеты основаны на данных, отображаемых на некоторых основных экранах приложения.



Книги по умолчанию (Default Book) содержат следующие отчеты:
Start View Reports (Отчеты экрана Start) - Содержит отчеты, основанные на данных, отображаемых на экране Start. Прямой доступ к этим же отчетам можно получить с экрана Start, щелкнув кнопкой мыши на  (Просмотр отчетов) и выбрав любой из отчетов в меню списка.

Channel View Reports (Отчеты экрана Channel) - Содержит отчет, основанный на данных, отображаемых на экране Channel (Канал). Прямой доступ к этому же отчету можно получить с экрана Channel (Канал), щелкнув кнопкой мыши на  и выбрав Selected Channel (Выбранный канал) или All Channels (Все каналы) в меню списка.

Interference View Reports (Отчеты экрана помех) - Содержит отчет, основанный на данных, отображаемых на экране Interference (Помехи). Прямой доступ к этому же отчету можно получить с экрана Interference (Помехи), щелкнув кнопкой мыши на  и выбрав Interference (Помехи) в меню списка.

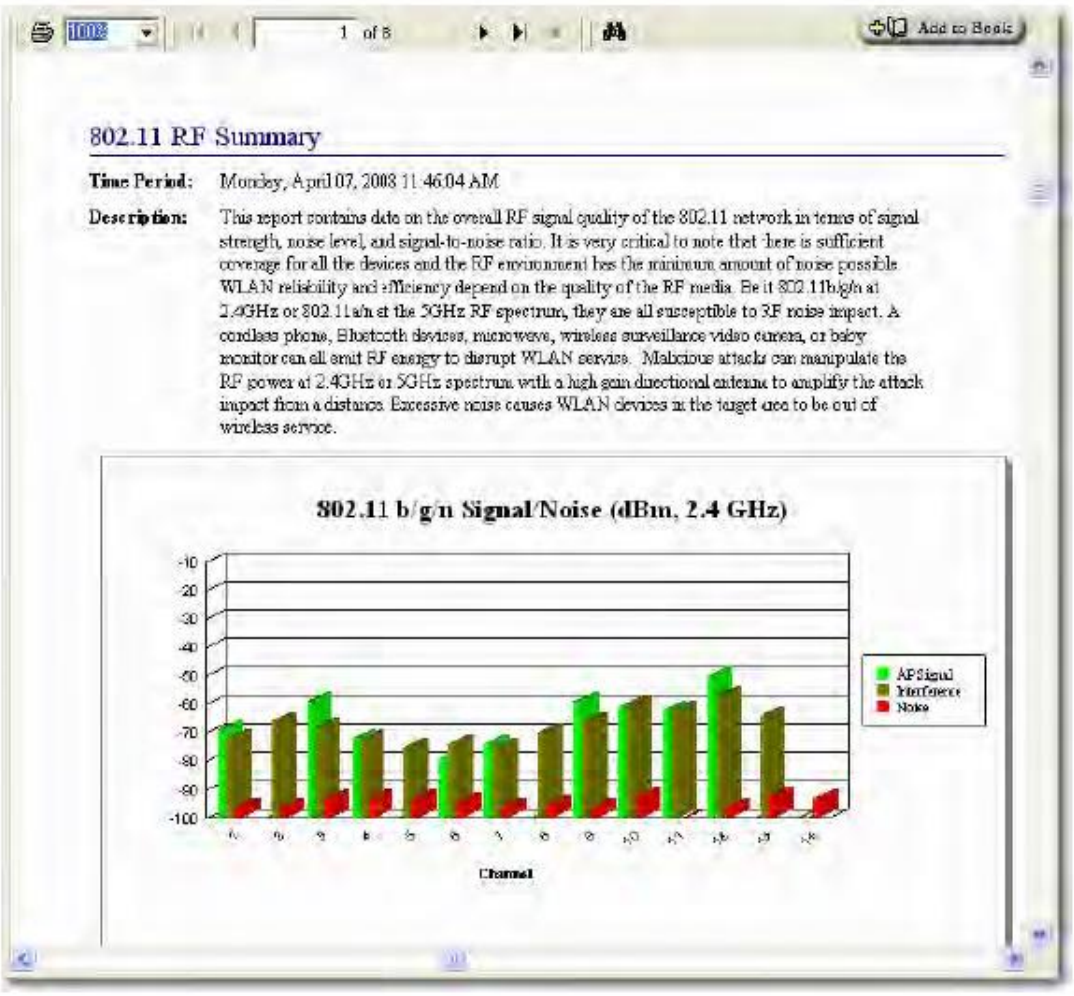
Infrastructure Reports (Отчеты экрана инфраструктуры) - Содержит отчет, основанный на данных, отображаемых на экране Infrastructure (Инфраструктура). Прямой доступ к этому же отчету можно

получить с экрана Infrastructure (Инфраструктура), щелкнув кнопкой мыши на  и выбрав Selected Device (Выбранное устройство) или Hierarchy Summary (Сводка иерархии) в меню списка.

Alarm Detail Reports (Отчеты подробностей о сигналах тревоги) - Содержит отчеты, основанные на подробных данных о сигналах тревоги, отображаемых на экране AirWISE. Прямой доступ к этому же отчету можно получить с экрана AirWISE, щелкнув кнопкой мыши на  и выбрав Alarm Detail (Сведения о тревоге), а затем любую из опций в меню списка.
Alarm Summary Reports (Сводные отчеты по сигналам тревоги) - Содержит отчеты, основанные на сводных данных по сигналам тревоги, отображаемым на экране AirWISE. Прямой доступ к этому же отчету можно получить с экрана AirWISE, щелкнув кнопкой мыши на  и выбрав Alarm Summary (Сводка тревог), а затем любую из опций в меню списка.
Chart View Device Reports (Отчеты по устройствам экрана диаграммы) - Содержит отчеты, основанные на данных об устройствах, захваченных в вашей сети.
Compliance Reports (Отчеты о соответствии) - Содержит отчеты, основанные на статусе соответствия вашей сети нормативным требованиям.

Панель отчетов

В правой части экрана Reports (Отчеты) находится панель отчетов, на которой отображается содержимое выбранного отчета. Панель отчета показана на рисунке ниже. Она предоставляет ряд инструментов для просмотра отчета. Обратитесь к разделу «Меню и инструменты экрана Reports (Отчеты)».

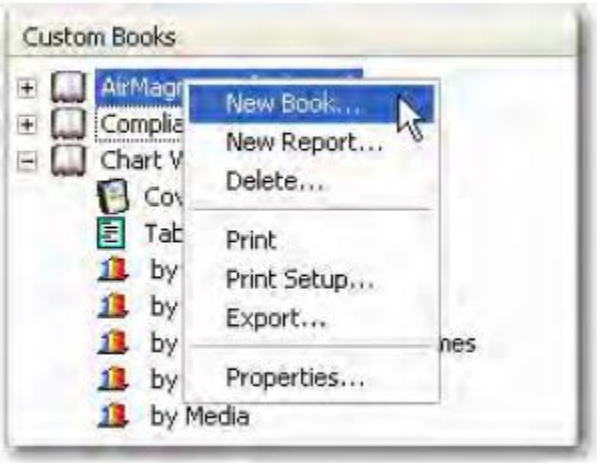


Создание книги отчетов

Книгу отчетов можно создать, используя настраиваемую титульную страницу, оглавление и отчеты по своему выбору. Это хороший способ классифицировать данные, обмениваться данными и архивировать данные, которые захватываются в вашей сети.

Для создания книги отчетов:

1. Щелкните правой кнопкой мыши на разделе Custom Books (Пользовательские книги), чтобы открыть контекстное меню.



2. В меню правой кнопки мыши выберите New Book… (Новая книга). Откроется диалоговое окно AirMagnet Report Book Detail (Сведения о книге отчетов AirMagnet).

3. В диалоговом окне AirMagnet Report Book Detail (Сведения о книге отчетов AirMagnet) сделайте необходимые записи и/или выбор, как описано в таблице ниже.

Запись/Выбор	Описание
Book Title (Название книги)	Название книги отчетов, отображаемое в разделе Custom Books (Пользовательские книги).
Table of Contents (Оглавление)	Если выбрано (отмечено), оглавление будет создано автоматически. Оглавление основано на добавленных в книгу отчетах, при этом каждый отчет представляет собой отдельную главу. Количество записей в оглавлении равно количеству отчетов, добавленных в книгу отчетов.

Cover Page (Обложка)	Если выбрано (отмечено), в книгу отчетов будет автоматически добавлена обложка. Обложка (титульная страница) содержит описанную ниже информацию.
Main Title (Основной заголовок)	Основной заголовок отображается в верхней части титульной страницы.
Subtitle (Подзаголовок)	Подзаголовок отображается на титульной странице под основным заголовком. Он призван помочь объяснить основной заголовок.
Company Information (Информация о компании)	Информация о предприятии, которому принадлежит беспроводная сеть.
Author (Автор)	Имя человека, создавшего книгу отчетов.

4. Нажмите кнопку ОК. Название книги (с обложкой и оглавлением) отобразится в разделе Custom Books (Пользовательские книги).

Примечание: На этот момент созданная вами книга отчетов не содержит отчетов. Для заполнения нужно добавить в книгу отчеты. Существует несколько способов добавления отчетов в книгу.

Добавление отчетов в книгу

Существует несколько способов добавления отчетов в книгу. Процедуры добавления отличаются друг от друга, как описано ниже.

Добавление открытого отчета в книгу

При использовании этой процедуры в книгу отчетов добавляет отчет, открытый в данный момент в окне отчетов.

Чтобы добавить открытый отчет в книгу отчетов:

1. В разделе Default Books (Книги по умолчанию) щелкните кнопкой мыши на нужном отчете, чтобы открыть его.
2. В разделе Custom Books (Пользовательские книги) выделите заголовок книги отчетов, в которую нужно добавить отчет.
3. Щелкните кнопкой мыши на 

.

Добавление в книгу отчетов по умолчанию

В этом разделе описываются процедуры прямого добавления отчетов в книгу путем их перетаскивания с помощью мыши.

Чтобы добавить отчеты в книгу отчетов:

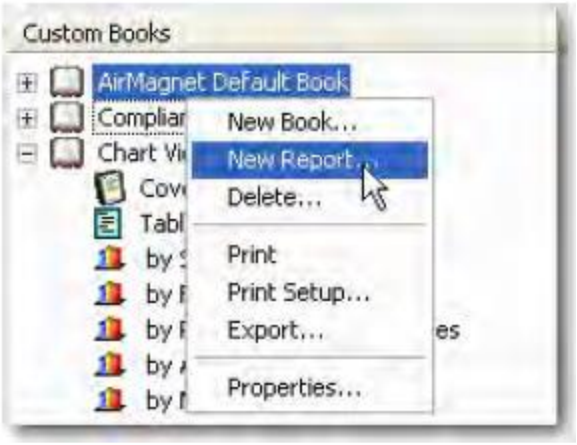
1. В разделе Default Books (Книги по умолчанию) выберите нужный отчет и перетащите его прямо в книгу.
2. Повторяйте шаг 1, пока в книгу не будут добавлены все необходимые отчеты.

Добавление пользовательских отчетов в книгу

В этом разделе описываются процедуры добавления в книгу отчетов пользовательских отчетов. Этот метод отличается от других методов тем, что позволяет настраивать отчеты перед их добавлением в книгу отчетов.

Для добавления пользовательского отчета в книгу отчетов:

1. В разделе Custom Books (Пользовательские книги) щелкните правой кнопкой мыши на названии нужной книги. Появится контекстное меню.



2. В меню правой кнопки мыши выберите New Report… (Новый отчет). Откроется диалоговое окно AirMagnet Report Detail (Подробности отчета AirMagnet).

3. В поле Report Type (Тип отчета) щелкните кнопкой мыши на направленной вниз стрелке, чтобы открыть список отчетов, и выберите тип отчета в разворачивающемся меню.

Примечание: С этого момента диалоговое окно может выглядеть по-разному в зависимости от выбранного отчета. Некоторые отчеты содержат больше фильтров, чем другие.

4. Следуйте инструкциям на экранах, если они имеются, для точной настройки выбранного отчета.
5. Нажмите кнопку OK. Пользовательский отчет добавляется в книгу отчетов.
6. Повторяйте шаги с 1 по 5, чтобы добавить в книгу все необходимые пользовательские отчеты.

Изменение свойств книги

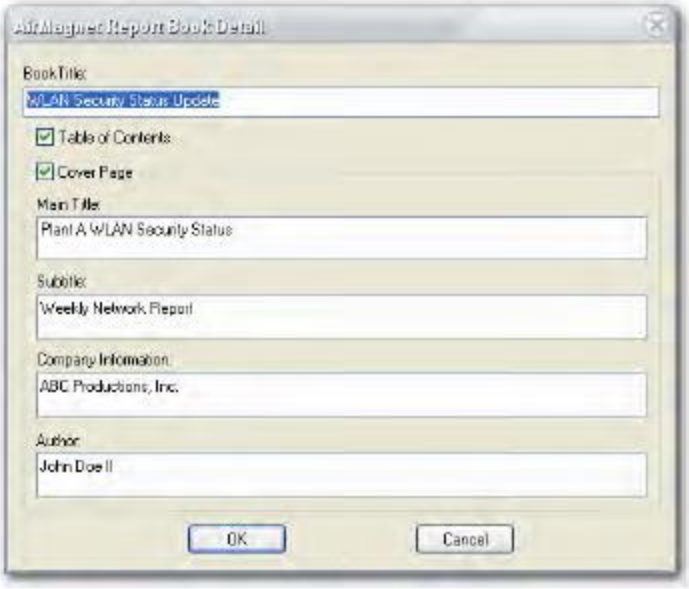
Изменение свойств книги отчетов подразумевает внесение изменений в информацию на ее титульной странице.

Примечание: Данная возможность относится только к книгам отчетов в разделе Custom Books (Пользовательские книги).

Для изменения свойств книги отчетов:

1. В разделе Custom Books (Пользовательские книги) щелкните правой кнопкой мыши на нужной книге отчетов.

2. В меню правой кнопки мыши выберите Properties… (Свойства). Откроется диалоговое окно AirMagnet Report Book Detail (Сведения о книге отчетов AirMagnet).



3. Внесите желаемые изменения и нажмите кнопку OK.

Изменение содержимого книги

Изменение содержимого книги отчетов означает внесение изменений в данные, содержащиеся в отчете, с помощью различных фильтров.

Для изменения содержания отчета:

1. В разделе Custom Books (Пользовательские книги) щелкните правой кнопкой мыши на нужном отчете.

2. В меню правой кнопки мыши выберите Properties… (Свойства). Откроется диалоговое окно AirMagnet Report Detail (Сведения об отчете AirMagnet).

3. Внесите желаемые изменения и нажмите кнопку ОК.

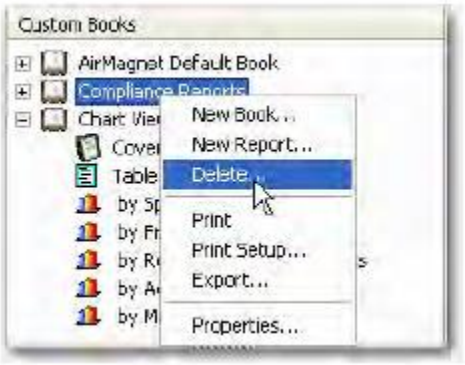
Удаление отчета или книги отчетов

По мере создания новых книг отчетов раздел Custom Books (Пользовательские книги) может переполниться. Для очистки этой части пользовательского интерфейса можно удалить те отчеты или книги отчетов, которые уже устарели.

Примечание: Отчеты или книги отчетов можно удалять только в разделе Custom Books (Пользовательские книги); из раздела Default Books (Книги по умолчанию) ничего нельзя удалить.

Чтобы удалить отчет из книги отчетов:

1. В разделе Custom Books (Пользовательские книги) щелкните правой кнопкой мыши на отчете или книге отчетов. Появится контекстное меню.



2. В меню правой кнопки мыши выберите Delete… (Удалить). Появится окно подтверждения.
3. Нажмите Yes (Да).

Печать отчета

Любой отчет или книгу отчетов из раздела Default Books (Книги по умолчанию) или из раздела Custom Books (Пользовательские книги) на экране Reports (Отчеты) можно распечатать.

Для печати отчета (из Default Books (Книги по умолчанию) или Custom Books (Пользовательские книги)):

1. Откройте нужный отчет.
2. Щелкните кнопкой мыши на  (Печать отчета).

Примечание: Приведенные выше инструкции применимы к печати отчета из раздела Default Books (Книги по умолчанию) или Custom Books (Пользовательские книги). Также отчеты можно распечатать из раздела Custom Books, используя меню правой кнопки мыши.

Для печати отчета (только из раздела Custom Books (Пользовательские книги)):

3. В разделе Custom Books (Пользовательские книги) щелкните правой кнопкой мыши на нужном отчете.

4. В меню правой кнопки мыши выберите Print (Печать).

Примечание: Меню правой кнопки мыши доступно только в разделе Custom Books (Пользовательские книги) экрана Reports (Отчеты).

Экспортирование отчета

Отчеты или книги отчетов в разделе Custom Books (Пользовательские книги) экрана Reports (Отчеты) можно экспортировать в файлы любого из следующих форматов:

- Adobe PDF
- HTML
- MS Word
- XML

Для экспортирования пользовательского отчета или книги отчетов:

1. В разделе Custom Books (Пользовательские книги) щелкните правой кнопкой мыши на нужной записи.
2. В меню правой кнопки мыши выберите Export… (Экспортировать). Откроется диалоговое окно Export.

3. В диалоговом окне Export выберите формат файла, укажите путь для экспортирования и нажмите кнопку OK.

Просмотр отчета

Для просмотра любого отчета в разделе Default Books (Книги по умолчанию) или Custom Books (Пользовательские книги) списка отчетов просто щелкните на нем кнопкой мыши. Обратитесь к разделу «Панель отчетов».

Примечание: Время, необходимое для открытия отчета, зависит от его размера.

Использование инструмента поиска в отчете

Для текстового поиска в отчете используйте инструмент  (Search Text), который позволяет находить любые буквенно-цифровые символы или строки символов в тексте отчета.

Для поиска текста в отчете:

1. Откройте отчет на экране Report (Отчет).
2. Щелкните кнопкой мыши на  . Откроется диалоговое окно поиска.

3. Введите текст, который хотите найти, и нажмите Find Next (Найти далее).
4. Если текст доступен, программа найдет его и выделит на экране отчета.
5. Для продолжения поиска нажимайте Find Next (Найти далее), пока не дойдете до конца отчета.

Отчеты о соответствии

Отчеты о соответствии предоставляют наглядную сводку соответствия вашей сети различным отраслевым стандартам.

Примечание: Отчеты о соответствии PCI Compliance Report и HIPAA Compliance Report можно использовать в качестве введения резюме для руководства (Executive Summaries) для соответствующих отчетов или в качестве автономных отчетов Executive Summary.

Отказ от ответственности

Обратите внимание, что ответственность за соблюдение применимых законов и правил несут клиенты AirMagnet. Хотя отчеты о соблюдении политик AirMagnet (AirMagnet Policy Compliance Reports) содержат информацию о законе и призваны помочь вам соблюдать государственные постановления, такая информация не является юридической консультацией, и вы несете единоличную ответственность за получение консультации компетентного юриста относительно идентификации и толкования любого закона или постановления.
Важный отказ от ответственности: Компания NetAlly не заявляет и не гарантирует, что ее услуги, продукты или любая другая информация, которую она предоставляет клиенту, обеспечит соблюдение вами любого закона или постановления.

Типы отчетов о соответствии

Директива Министерства обороны 8100.2
Директива министерства обороны США (МО) за номером 8100.2 (далее «директива») объединяет основные разделы стратегии в отношении использования коммерческих беспроводных устройств, услуг и технологий в МО. Ее цель состоит в защите сетей МО от уязвимостей, присущих беспроводным сетям, что делает безопасность обязательным предварительным условием для развертывания и использования коммерческих беспроводных технологий в МО.

Закон о преемственности и подотчетности медицинского страхования (HIPAA, США)
Закон HIPAA был принят в целях повышения эффективности национальной системы здравоохранения и содействия использованию в здравоохранении EDI (Electronic Data Interchange – электронный обмен данными). Для этого HHS (Department of Health and Human Services – министерство здравоохранения и социальных услуг) были выпущены правила защиты конфиденциальности и безопасности PHI (Protected Health Information – закрытая медицинская информация). Под PHI понимается любая медицинская информация, которая идентифицирует человека и относится к его или ее физическому или психическому здоровью.

Закон Грэма-Лича-Блили
Закон Грэма-Лича-Блили (GLBA), также известный как «Закон о модернизации финансовой системы 1999 года», гласит, что финансовые институты защищают безопасность и конфиденциальность личной финансовой информации своих клиентов.

Закон Сарбейнса-Оксли
Закон Сарбейнса-Оксли (SOX), также известный как «Закон о реформе учета и отчетности в открытых компаниях и защите интересов инвесторов» был принят Конгрессом США в 2002 году как всеобъемлющее законодательство по реформированию бухгалтерского учета, раскрытия финансовой информации и корпоративного управления публичных компаний.

Стандарт Payment Card Industry Data Security Standard
Стандарт PCI DSS (Payment Card Industry Data Security Standard – стандарт защиты информации в индустрии платежных карт) версии 3.0 призван заменить версию 2. AirMagnet включает отчеты о соответствии стандартам PCI 2.0 и 3.0.
Эти отчеты о соответствии содержат информацию, которая помогает оценщику определить, соответствует ли организация стандарту требований PCI DSS, применимому к беспроводным сетям и устройствам, работающим на нерегулируемых радиочастотных диапазонах (от 2,4 до 5 ГГц).

Соглашение Basel II
Базельское соглашение по капиталу (Basel II) позволяет еще больше согласовать подход банков и банковских регуляторов к управлению рисками. Оно предназначено для создания минимального уровня капитала в международных банках. В отношении конкретных требований к AirMagnet, Basel II включает явные требования к капиталу для покрытия операционного риска. Операционный риск включает в себя риски в области безопасности в работе с беспроводными сетями. Соглашение Basel II является результатом развития Базельского соглашения Basel I. Они оба были разработаны Базельским комитетом по банковскому надзору (далее «комитет»). Комитет состоит из органов банковского надзора и центральных банков Группы десяти стран (G10) . К странам G10 относятся: Бельгия, Канада, Франция, Германия, Италия, Япония, Люксембург, Нидерланды, Испания, Швеция, Швейцария, Великобритания и Соединенные Штаты. Международные банки могут использовать продукты AirMagnet и отчеты о соответствии (Compliance Reports™) для выявления и смягчения операционных рисков при использовании беспроводных сетей.

Директива EC CRD/CAD3
Директива Европейского союза о требованиях к капиталу (European Union Capital Requirements Directive), более известная как CAD3 (Capital Adequacy Directive – директива о достаточности капитала), реализует Базельское соглашение II и вводит новые требования к капиталу для международных банков, кредитных учреждений и инвестиционных компаний в ЕС. Она является развитием предыдущей директивы, которая реализовывала требования к капиталу, входившие в Базельское соглашение I. Отчеты об уровне соответствия для системы AirMagnet и для устройств определяют операционные риски в беспроводных сетях, которые могут привести к сбоям или неисправностям системы и мошенническим действиям извне.

Стандарт ISO 27001
Стандарт ISO/IEC 27001:2005 (далее ISO 27001) является международным стандартом, предназначенным для организаций любого размера и типа (государственных и негосударственных). В базе международный стандарт следует использовать в качестве модели для построения системы менеджмента информационной безопасности (International Security Management System - ISMS). ISMS является частью организационной системы, которая управляет сетями и системами. Она основывается на рисках бизнеса и направлена на «создание, внедрение, эксплуатацию, мониторинг, обзор, поддержку и улучшение информационной безопасности». Выходя за пределы модели, организации могут получить сертификацию ISO 27001 у независимых аудиторов. Сертификация способна продемонстрировать стремление организаций к обеспечению безопасности и помочь завоевать доверие партнеров и клиентов. Также ее можно использовать в качестве доказательства соответствия законодательным требованиям, хотя сама по себе она не будет удовлетворять требованиям законодательства. Соответствие организации стандарту ISO 27001 удостоверяют такие независимые аудиторы, как ISOQAR и LRQA. Обратите внимание, что аудиторов ISO 27001 регулируют Американское национальное бюро аккредитации (ANAB) и Служба аккредитации Соединенного Королевства. AirMagnet удовлетворяет требованиям стандартов ISO 27001 и 17799 для беспроводных сетей и устройств с отчетами о соответствии на уровне системы, политики и конкретных устройств. Благодаря использованию модели ISO 27001 Plan-Do-Check-Act, решения AirMagnet способны помочь организации спланировать, проверить и действовать в направлении улучшения ISMS.

Закон FISMA
Закон FISMA (Federal Information Security Management Act – федеральный закон США об управлении информационной безопасностью) требует, чтобы такие федеральные ведомства, как Министерство

здравоохранения и социальных услуг, Федеральная комиссия связи (FCC) и Федеральная торговая комиссия (FTC) разработали, задокументировали и внедрили программу информационной безопасности для обеспечения безопасности информации и информационных систем, которые поддерживают деятельность и активы федеральных учреждений. Сюда также включаются информация и информационные системы, предоставляемые агентству от другого агентства или подрядчика.

Закон FISMA применяется к следующему:

- Вся информация федерального правительства, за исключением информации, имеющей гриф секретности.
- Все информационные системы, за исключением тех, которые функционируют как системы национальной безопасности.
- Любая организация, которая является государственным органом, продает оборудование и/или программное обеспечение государственным органам или поддерживает информацию или информационные системы государственного органа.

Настройка отчетов о соответствии

Если данные, представленные в предоставляемых AirMagnet отчетах о соответствии, не соответствуют требованиям вашей корпоративной сети, вы можете настроить информацию, используемую отчетом о соответствии каждого типа. Возможность настройки конкретной информации отчета может помочь пользователям привести систему отчетов в соответствие потребностям компании.

Для настройки данных отчета о соответствии:

1. На экране Reports (Отчеты) консоли щелкните кнопкой мыши на  (Настроить отчет о соответствии). Откроется диалоговое окно Configure Compliance Report (Настроить отчет о соответствии).

2. Используйте разворачивающийся список в верхней части окна для выбора настраиваемого отчета о соответствии. На нижней панели отображаются все разделы выбранного отчета.
3. Чтобы развернуть каждый раздел, используйте опцию «+» (раскрыть). Это покажет сигналы тревоги по каждому из разделов.
4. Снимите метки из полей тех тревог, которые не следует включать в отчет.
5. Нажмите Apply (Применить), чтобы сохранить изменения, затем нажмите кнопку ОК, чтобы закрыть диалоговое окно.

Диапазон 49 ГГц

О диапазоне 4,9 ГГц

С начала 2003 года Федеральная комиссия по связи (FCC) выделила радиочастотный спектр шириной 50 МГц в диапазоне 4,9 ГГц (то есть между 4,940 МГц и 4,990 МГц) для использования в целях общественной безопасности. Использование спектра 4,9 ГГц лицензируется; связь в этом радиочастотном диапазоне должна обеспечивать защиту жизни, здоровья или имущества населения. Соответствующие государственные или местные органы власти могут иметь лицензии на использование частотного диапазона 4,9 ГГц в пределах своей юрисдикции. Организации, которые не имеют права на получение лицензий, но предоставляют услуги, критически важные для поддержки общественной безопасности, могут совместно использовать лицензии с держателями лицензий на диапазон 4,9 ГГц. Недавно выделенный спектр позволяет службам общественной безопасности быстро развертывать на месте происшествия беспроводные сети для потоковой передачи видео, мгновенного доступа в сеть Интернет и обеспечения доступа к базам данных, а также быстрой передачи больших объемов данных или файлов изображений, таких как карты, чертежи зданий, медицинские записи пациентов и фотографии.

Правила FCC делят использование диапазона 4,9 ГГц на первичное и вторичное. Первичное включает точки доступа, временные фиксированные соединения «точка-точка» или «точка-многоточка» для базовых/мобильных/портативных операций; ко вторичному относятся операции с фиксированным соединением «точка-точка», которые являются вторичными относительно основного использования этой полосы частот.

Лицензия дает право агентству общественной безопасности использовать все 50 МГц спектра в пределах своей юрисдикции. Разные лицензиаты, работающие в непосредственной близости друг от друга, используют все частоты совместно; они несут ответственность за предотвращение, уменьшение и устранение помех. В Правилах также указано, что ни при каких обстоятельствах вторичное использование спектра не должно мешать его первичному использованию. С другой стороны, вторичные операции должны выдерживать помехи, вызванные первичными операциями.

Мониторинг диапазона 4,9 ГГц

В качестве лицензированного радиочастотного диапазона наибольшее преимущество диапазона 4,9 ГГц заключается в том, что он обеспечивает свободную от помех рабочую среду для широкополосной связи в сфере общественной безопасности. Он лучше всего подходит для фиксированных беспроводных приложений организации связи точка-точка (P2P) и точка-многоточка (PMP).
При использовании в режимах P2P и PMP существует ряд услуг, которые агентство общественной безопасности может создавать на базе магистральной радиопередачи 4,9 ГГц. Эти услуги и приложения могут заменять дорогостоящие арендуемые услуги, что приведет к окупаемости инвестиций и долгосрочной экономии для агентства. Приложение AirMagnet WiFi Analyzer - первое программное приложение, способное проводить мониторинг и анализ в частотном диапазоне 4,9 ГГц.

Поддерживаемые адаптеры беспроводной сети 4,9 ГГц

Для использования функции 4,9 ГГц приложения AirMagnet WiFi Analyzer необходим один из следующих адаптеров беспроводной сети диапазона 4,9 ГГц:

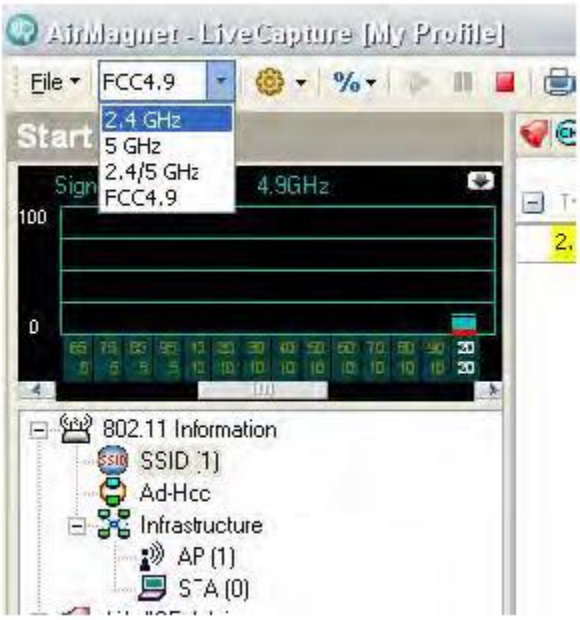
- Linksys Wireless A+G Notebook Adapter WPC55AG версии 1.3
- Ubiquiti SR4C 4.9 GHz
- TRENDnet TEW-501PC ag

Настройка приложения AirMagnet WiFi Analyzer в режиме 4,9 ГГц

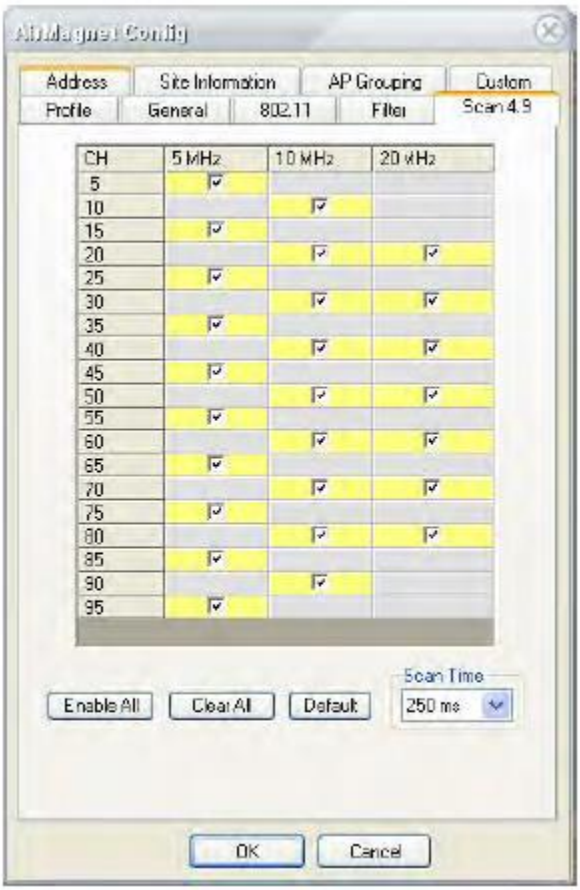
Для переключения приложения AirMagnet WiFi Analyzer в режим 4,9 ГГц:

1. Вставьте поддерживаемый адаптер беспроводной сети диапазона 4,9 ГГц в слот для карт на своем портативном компьютере.
2. Запустите приложение AirMagnet WiFi Analyzer.

3. На панели меню нажмите кнопку Band (Диапазон) и в разворачивающемся списке выберите FCC 4.9. Смотрите рисунок ниже.



4. Щелкните кнопкой мыши на File > Config… > Scan 4.9 (Файл > Настроить... > Сканировать 4.9). Смотрите рисунок ниже.

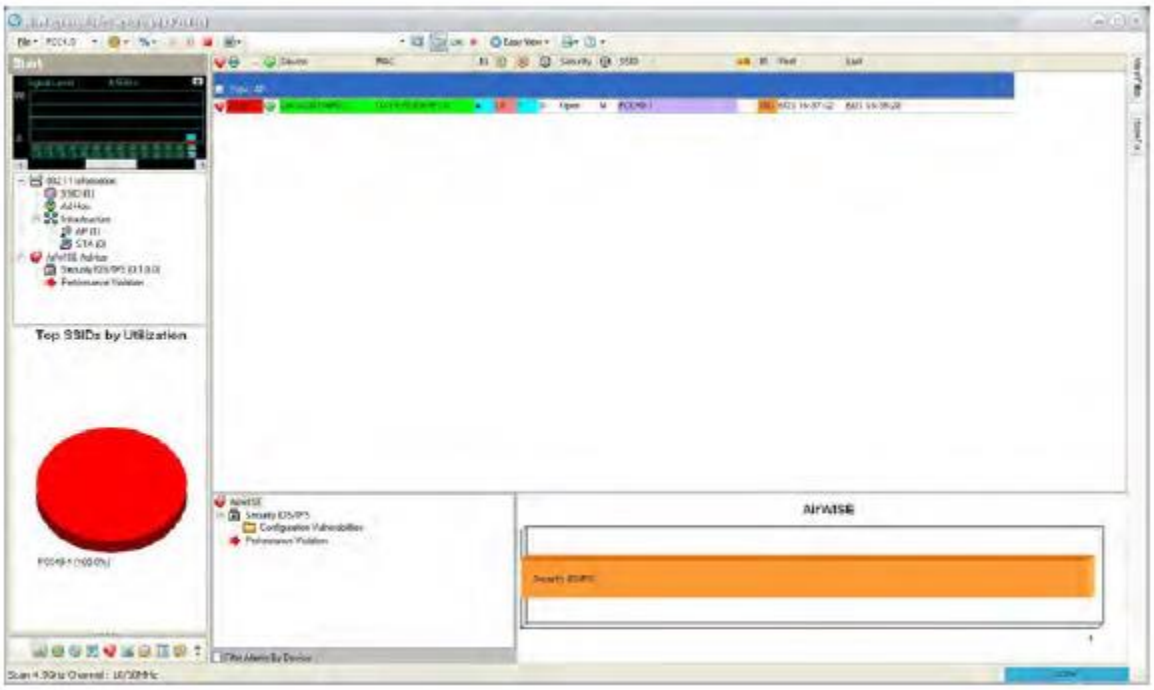


Примечание: На приведенном выше рисунке показаны все каналы частотного диапазона 4,9 ГГц, выделенные в США для сферы общественной безопасности.

5. Выберите желаемые каналы и полосы пропускания 4,9 ГГц.
6. Укажите время (интервал) сканирования (Scan Time).

7. Нажмите кнопку ОК.

Примечание: Когда приложение AirMagnet WiFi Analyzer работает в режиме 4,9 ГГц, на его экранах отображаются только данные, обнаруженные на выбранных каналах диапазона 4,9 ГГц. Объем отображаемых на экране данных зависит от количества устройств диапазона 4,9 ГГц, работающих в вашей сети. На рисунке ниже показан экран Start в режиме 4,9 ГГц.



Устранение проблем 802.11n

Об устранении проблем 802.11n

В этом разделе рассказывается, как использовать приложение AirMagnet WiFi Analyzer для мониторинга, поиска и устранения неисправностей и устранения сетевых проблем, связанных со стандартом 802.11n.

- Как узнать особенности 802.11n на точке доступа?
- Какие функции 802.11n НЕ используются на точке доступа (AP) или станции (STA)?
- Что произойдет, если определенная функция 802.11n (не) используется?
- Какой объем трафика передается при ширине канала 40 МГц?
- Какие настройки канала следует использовать, если у меня новая точка доступа?
- Как узнать максимальную пропускную способность установленной точки доступа?
- Почему я НЕ получаю ожидаемую пропускную способность от точки доступа?
- Какова ожидаемая пропускная способность устройства для точки доступа?
- Что следует учитывать при настройке новых точек доступа?
- Какое изменение пропускной способности сети ожидается при развертывании новых точек доступа и/или станций в сети?
- Как узнать пропускную способность сети между точкой доступа и станцией?
- Как узнать, связана ли моя точка доступа 802.11n с какими-либо устаревшими устройствами?
- Сколько служебных данных требует точка доступа 802.11n для поддержки устаревших устройств?
- Как связанные устаревшие устройства уменьшат пропускную способность устройства 802.11n?
- Сколько устаревших точек доступа можно добавить в сеть 802.11n?
- Как станции 802.11n влияют на существующую сеть 802.11a?

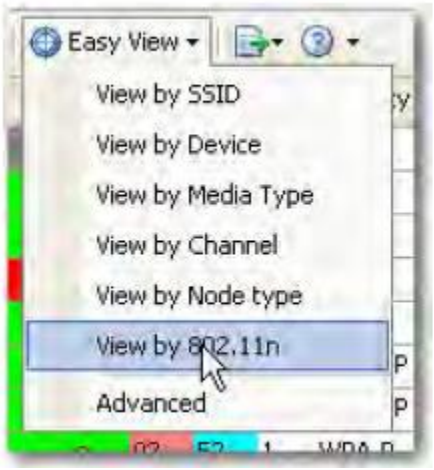
Как узнать особенности 802.11n на точке доступа?

Стандарт IEEE 802.11n содержит множество новых функций. Согласно IEEE, некоторые функции являются обязательными, в то время как другие необязательны. Чтобы в полной мере воспользоваться преимуществами нового протокола 802.11n, важно знать, какие функции 802.11n используются на точках доступа 802.11n, развернутых в вашей сети. Приложение AirMagnet WiFi Analyzer предлагает пользователю инструмент для этого.

Чтобы узнать о функциях 802.11n, используемых на точке доступа:

1. Откройте экран Start.
2. На панели меню щелкните кнопкой мыши на 

и в разворачивающемся меню выберите View by 802.11n (Просмотр по 802.11n).



Экран Start обновится и будет отображать только устройства 802.11n. Экран можно прокручивать вверх или вниз для просмотра всех точек доступа 802.11n в сети, а также влево и вправо для просмотра функции 802.11n и того, какие функции на каких точках доступа используются.

Примечание: Чтобы упростить получение информации обо всех доступных функциях 802.11n и о том, какие из этих функций используются на вашей точке доступа, можно открыть диалоговое окно Field Chooser (Выбор поля), щелкнув правой кнопкой мыши на экране Start и выбрав функцию Set Display Columns (Установить столбцы отображения). В этом диалоговом окне отображаются все типы данных, включая все функции 802.11n, которые в настоящий момент доступны для сети 802.11. Путем перетаскивания можно добавить все эти функции 802.11n на экран.

Выбор Easy View > View by 802.11n (Легкий просмотр > Просмотр по 802.11n) позволит отображать следующие функции 802.11n:

- Operating Mode (Режим работы)
- Primary/Secondary Channels (Первичные/вторичные каналы)
- RIFS Mode (Режим RIFS)
- SGI
- Non-Greenfield STAs Present (Наличие станций, не поддерживающих Greenfield)
- OBSS Non-HT STAs Present (Наличие станций OBSS Non-HT)
- Non-HT OBSS

- 40 MHz Tolerant (Толерантность к 40 МГц)
- LDPC
- Tx Channel Width (Ширина канала передачи)
- Rx Channel Width (Ширина канала приема)
- PCO
- Greenfield Supported (Поддерживается Greenfield)
- Tx STBC
- Rx STBC
- SM Power Save (Экономия энергии SM)
- Dual Beacon (Двойной маяк)
- Dual CTS Protection (Двойная защита CTS)

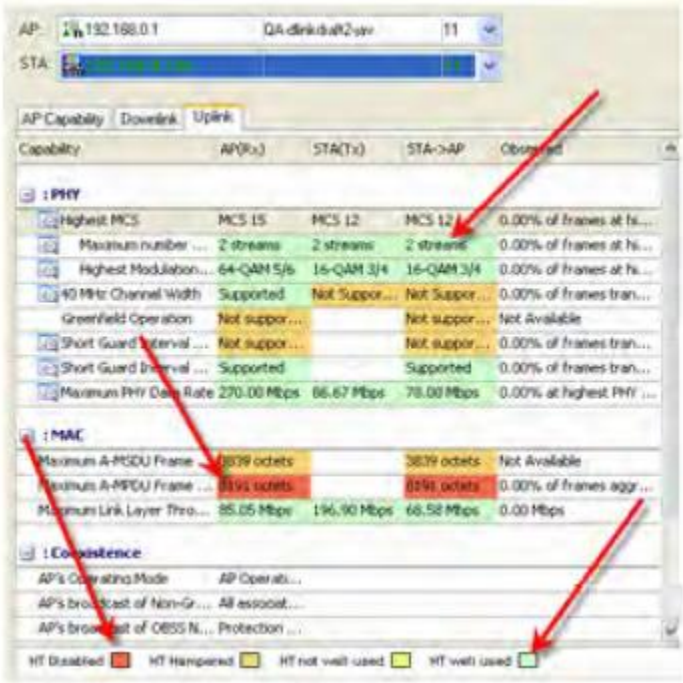
Примечание: Быстрое определение или объяснение любого из этих терминов можно получить, просто включив всплывающую подсказку (Bubble Help), щелкнув кнопкой мыши на  на панели меню. После включения всплывающей подсказки можно будет просто наводить указатель мыши на название любого столбца, чтобы получить для него всплывающую подсказку.

Какие функции 802.11n не используются на точке доступа (AP) или станции (STA)?

В настоящее время на рынке доступно множество точек доступа и станций с поддержкой 802.11n от разных производителей. Поскольку согласно IEEE некоторые функции 802.11n являются обязательными, а другие необязательными, важно иметь четкое представление обо всех устройствах 802.11n, развернутых в вашей сети. Прежде всего, необходимо знать, какие функции 802.11n поддерживаются или НЕ поддерживаются вашими устройствами 802.11n.

Чтобы узнать, какие функции 802.11n используются на ваших точках доступа или станциях 802.11n:

1. Откройте экран WiFi Tools (Инструменты WiFi), щелкнув кнопкой мыши.
2. Выберите инструмент Efficiency (Эффективность).



3. На экране Efficiency (Эффективность) выберите нужную точку доступа или станцию.

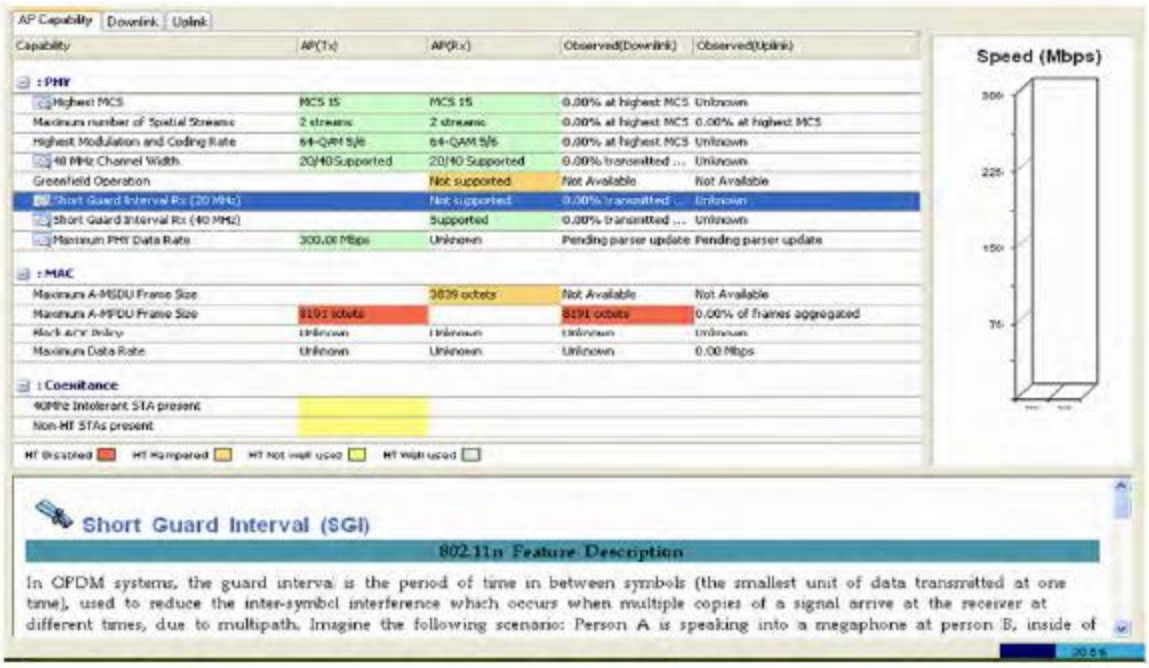
Примечание: Экран Efficiency (Эффективность) содержит подробное описание всех функций 802.11n в трех категориях: PHY, MAC и Coexistence. Инструкции по использованию экрана Efficiency приводятся в разделе «Анализ эффективности сети 802.11n».

Что произойдет, если определенная функция 802.11n (не) используется?

Все функции 802.11n будут иметь некоторое влияние на устаревшую сеть.

Чтобы узнать, как на вашу сеть повлияет использование или неиспользование определенной функции 802.11n:

1. Откройте экран WiFi Tools > Efficiency (Инструменты WiFi > Эффективность).
2. Используйте функцию AirMagnet 802.11n Learning Assistant, которая простым и понятным языком дает подробное объяснение каждой из ключевых функций 802.11n, ее преимуществ и недостатков, а также использования или неиспользования каждой из этих функций.



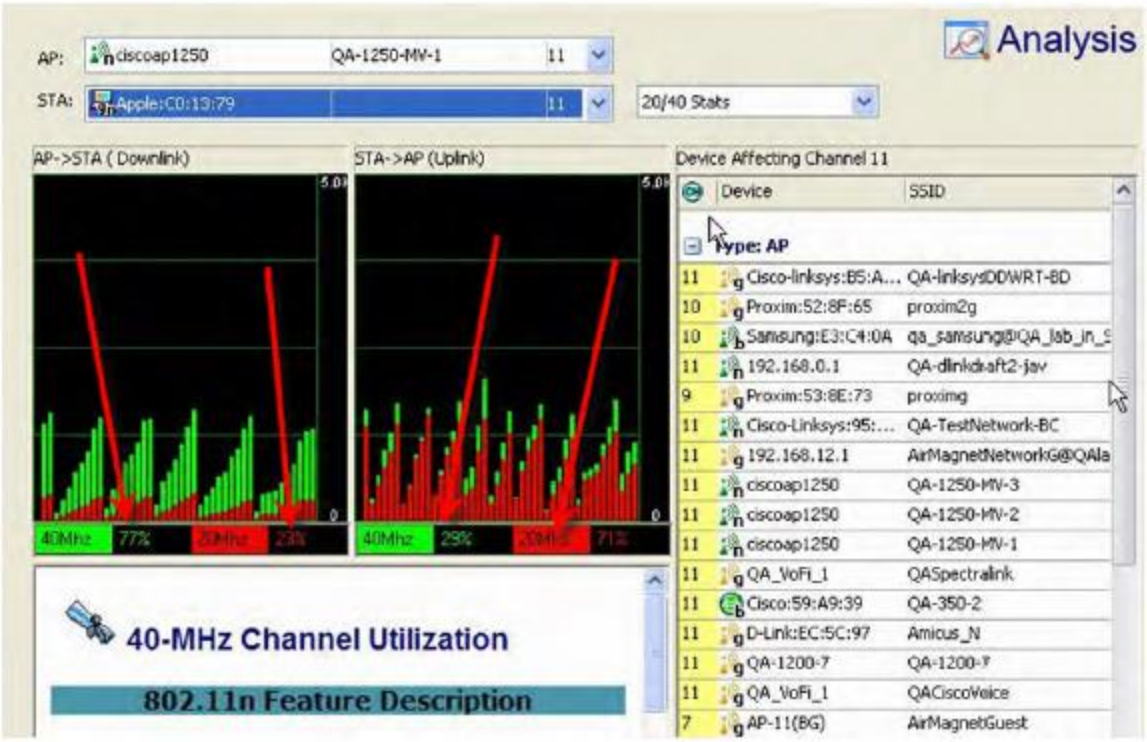
Какой объем трафика передается при ширине канала 40 МГц?

Протокол 802.11n поддерживает каналы 20 МГц и 40 МГц. Последний канал повышает эффективность работы сети.

Чтобы узнать, сколько трафика отправляется при ширине канала 40 МГц:

1. Откройте экран WiFi Tools (Инструменты WiFi).
2. Щелкните кнопкой мыши на инструменте Analysis (Анализ).
3. Выберите AP (Точка доступа) и STA (Станция).

4. Выберите 20/40 Stats (Статистика 20/40 МГц).



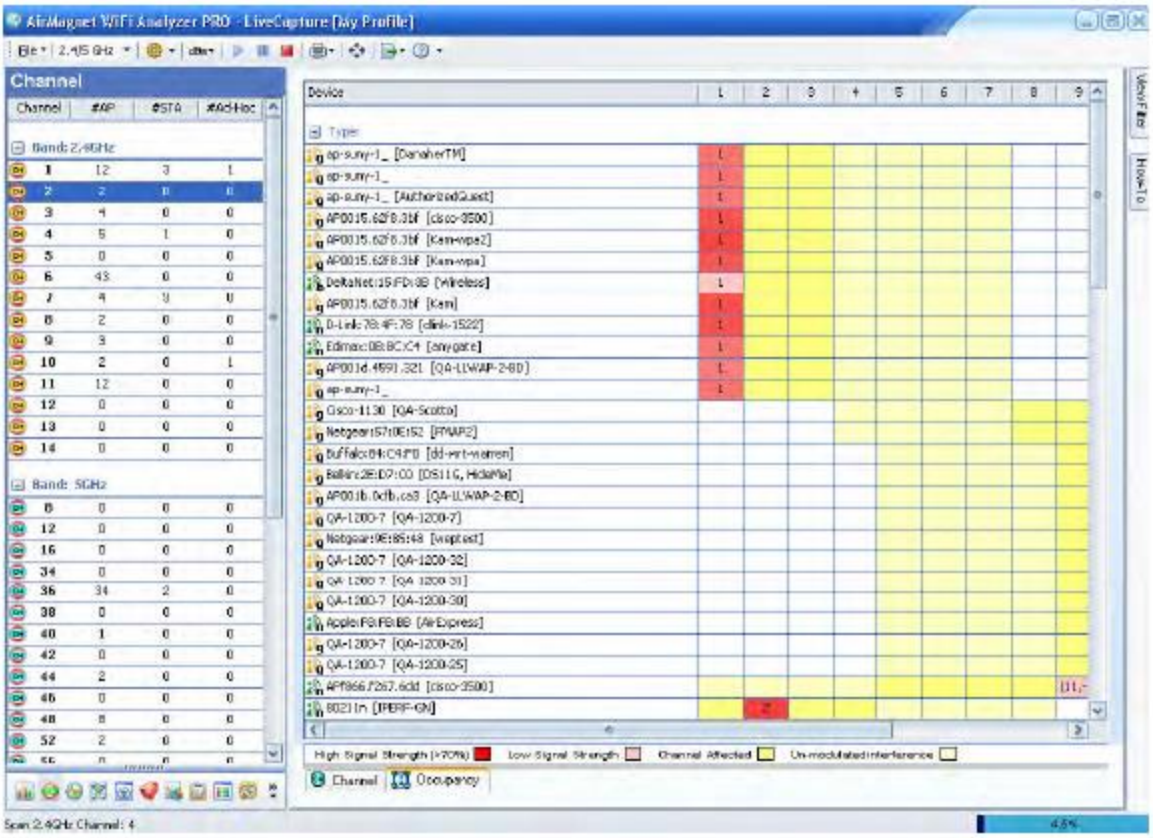
Примечание: На экране Analysis (Анализ) отображается процент (%) трафика 20 или 40 МГц между выбранной точкой доступа и станцией. Также на этом экране предоставлена статистика SGI, A-MPDU, MCS Index, PHY Data Rate Analysis и так далее. Для получения дополнительной информации обратитесь к разделу «Об инструментах 802.11n».

Какие настройки канала следует использовать, если у меня новая точка доступа?

По мере увеличения сетевых потребностей ваших сотрудников в сеть будут добавляться дополнительные точки доступа. Прежде чем устанавливать новую точку доступа в уже перегруженной сети, необходимо знать доступный оптимальный канал.

Чтобы узнать, какой канал лучше всего подходит для новой точки доступа:

1. Откройте экран Channel (Канал).
2. Откройте вкладку Occupancy (Занятость).



Примечание: На экране Channel/Occupancy (Канал/Занятость) представлен обзор с «высоты птичьего полета» использования радиочастотного спектра в сети. Показана центральная частота и использование модулированного и немодулированного спектра. Можно легко визуализировать занятые и/или незанятые каналы. Здесь предоставлена жизненно важная информация, необходимая для принятия обоснованного решения при планировании развертывания новых сетей или улучшения уже существующих.

Отображаемое на экране Channel/Occupancy (Канал/Занятость) состояние занятости всех доступных каналов поможет легко решить, какие каналы выбрать для новых точек доступа, развертываемых на перегруженной сети. Как правило, следует выбирать неиспользуемые каналы и избегать перегруженных каналов.

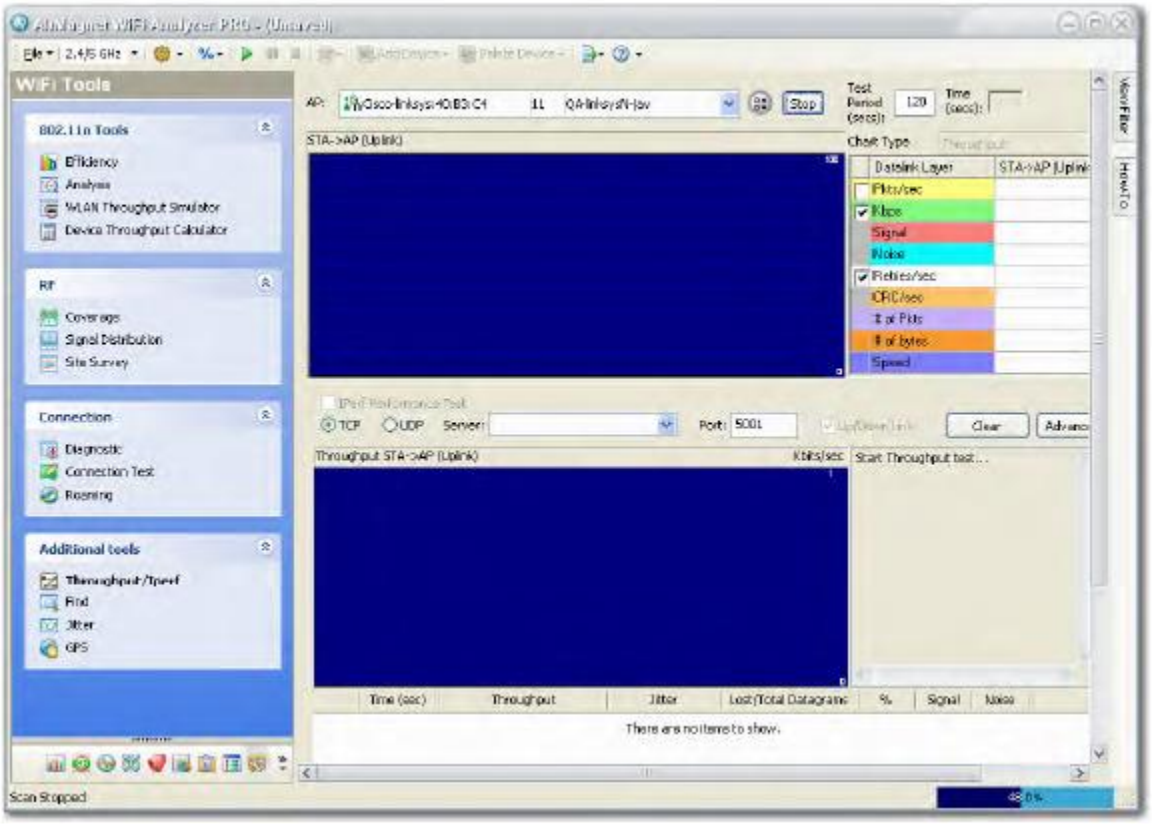
Как узнать максимальную пропускную способность установленной точки доступа?

Максимальную пропускную способность любой точки доступа, установленной в вашей сети, можно узнать с помощью инструмента Throughput/Iperf (Пропускная способность/Iperf) на экране WiFi Tools (Инструменты WiFi) приложения AirMagnet WiFi Analyzer.

Чтобы узнать максимальную пропускную способность точки доступа:

1. На экране WiFi Tools (Инструменты WiFi) щелкните кнопкой мыши на инструменте Throughput/Iperf (Пропускная способность/Iperf). Выберите точку доступа.
2. Укажите продолжительность периода тестирования (Test Period), например 120.
3. Выберите тип диаграммы (Chart Type), например, PHY Data Rate (Скорость передачи данных физического уровня).
4. Убедитесь, что стоит метка в поле Iperf Performance Test (Тестирование производительности Iperf).
5. Выберите TCP или UDP и укажите сервер (Server) и порт (Port).

6. Установите метку в поле Up/Downlink (Восходящий/нисходящий канал).
7. Щелкните кнопкой мыши на Start.



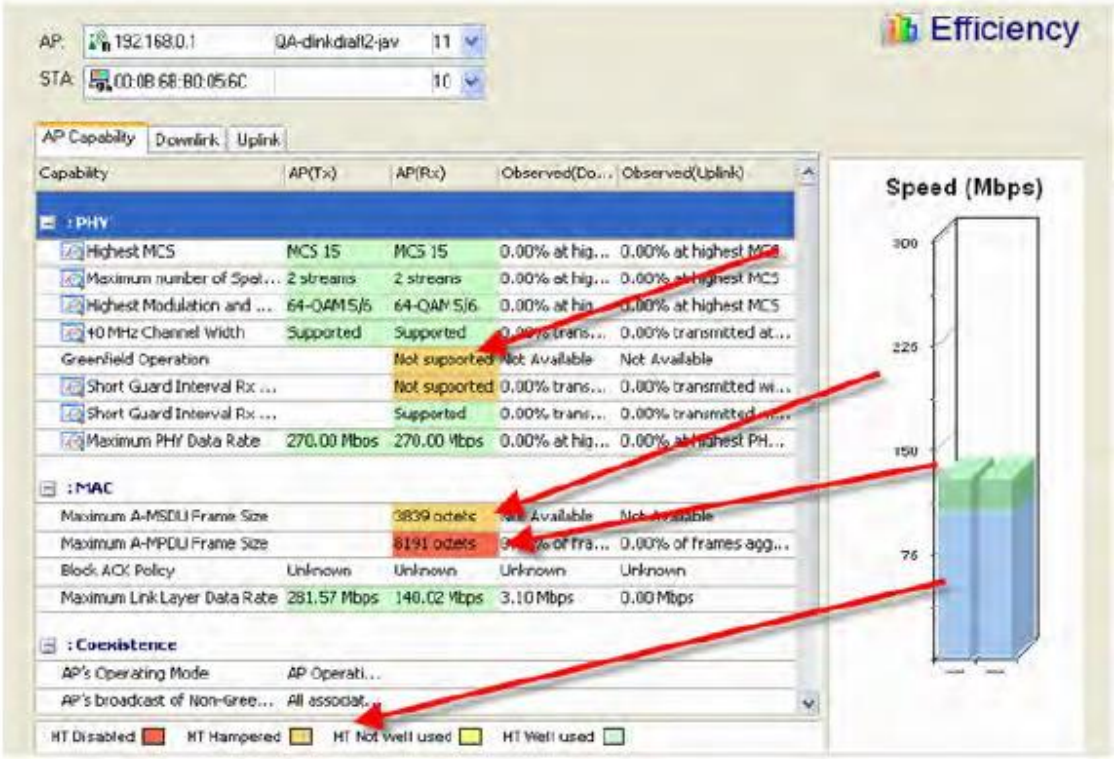
Примечание: На экране Throughput/Iperf (Пропускная способность/Iperf) отображается пропускная способность как восходящего, так и нисходящего каналов для выбранной точки доступа. Это позволяет протестировать производительность сети, используя протокол TCP или UDP. Он показывает различные факторы, такие как мощность сигнала, уровень шума, повторные попытки и ошибки CRC, которые могут повлиять на пропускную способность вашей сети. Для получения дополнительной информации обратитесь к разделу «Анализ полосы пропускания и пропускной способности сети с помощью Iperf».

Почему я не получаю ожидаемую пропускную способность от точки доступа?

Пропускная способность сети зависит от различных факторов. В результате пропускная способность вашей сети может колебаться в зависимости от динамики изменения сети.

Чтобы выяснить, почему вы не получаете ожидаемую пропускную способность от точки доступа:

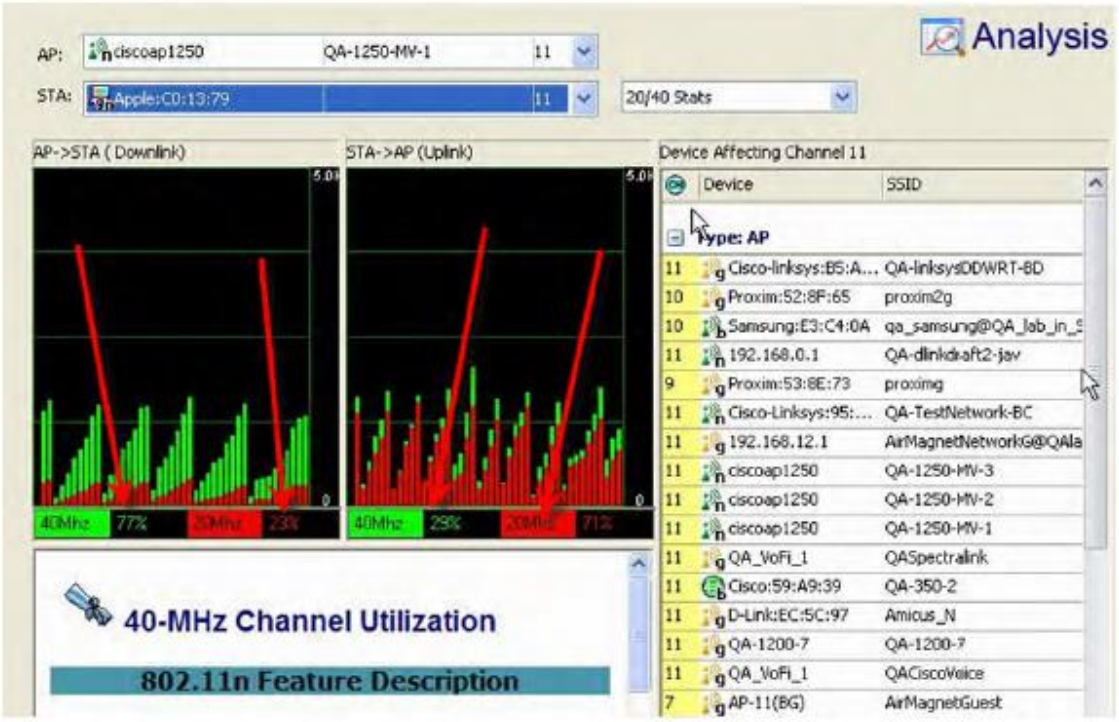
1. Откройте экран Efficiency (Эффективность).



Примечание: Инструмент Efficiency (Эффективность) позволяет анализировать транзакции между точками доступа и станциями. Внизу экрана располагается цветовая легенда, объясняющая, почему не достигается ожидаемая пропускная способность. Основываясь на этой информации, можно исправить ситуацию, включив настройки на своих устройствах 802.11n, которые позволят в полной мере использовать возможности HT-устройств 802.11n. Для получения дополнительной информации обратитесь к разделу «Эффективность 802.11n».

2. Откройте экран Analysis (Анализ).
3. Выберите точку доступа (AP) и станцию (STA).

4. Выберите 20/40 Stats (Статистика 20/40 МГц).



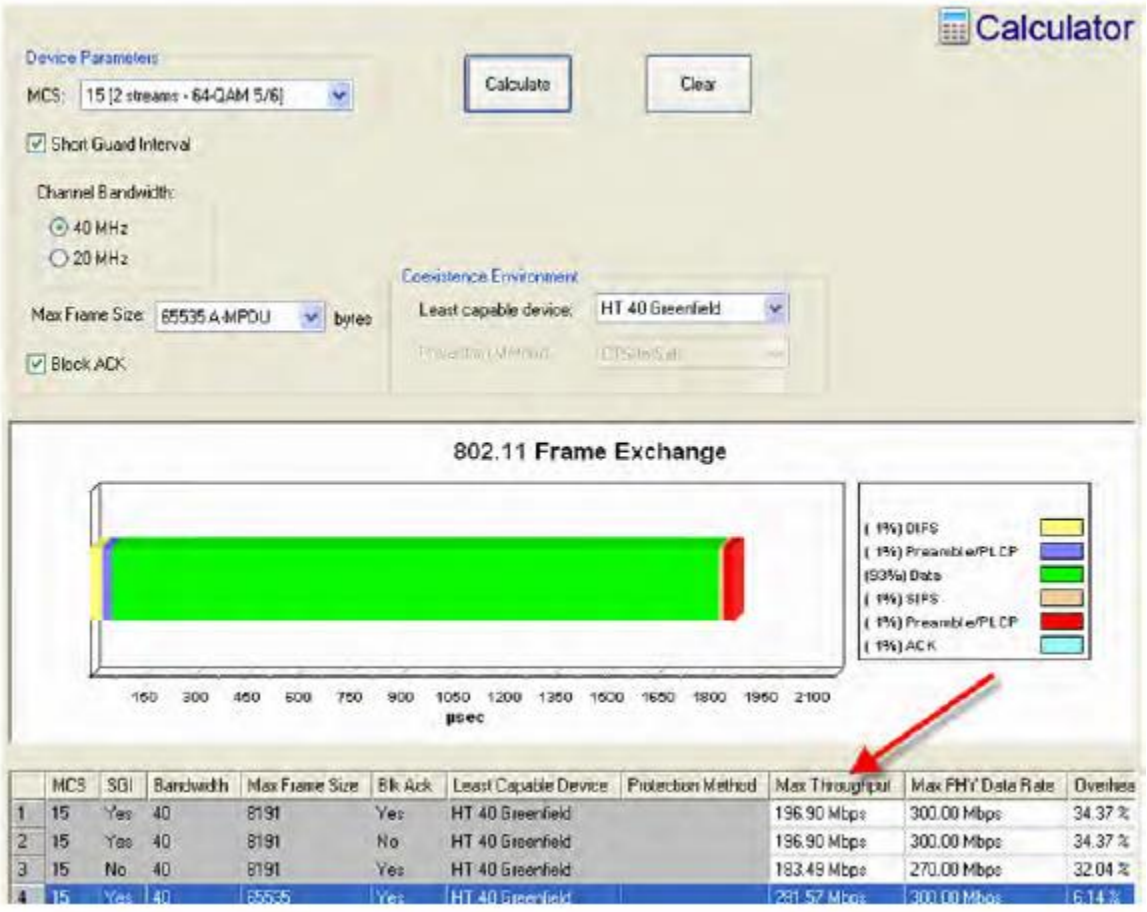
На экране отображается процент трафика, передаваемого по каналам 20 МГц и 40 МГц. Это позволяет определить, не является ли использование при более высокой скорости MCS низким. Также это указывает на низкое отношение сигнал-шум в шумных радиочастотных средах или на большое расстояние между точкой доступа и станцией.

Какова ожидаемая пропускная способность устройства для точки доступа?

Перед установкой точки доступа в сети желательно узнать уровень пропускной способности, который можно ожидать от точки доступа. Для этого можно использовать калькулятор пропускной способности устройства (Device Throughput Calculator) приложения AirMagnet WiFi Analyzer.

Для проверки ожидаемой пропускной способности устройства точки доступа:

1. Откройте экран Device Throughput Calculator (Калькулятор пропускной способности устройства) приложения AirMagnet WiFi Analyzer.
2. Задайте параметры, которые хотите использовать на точке доступа, и нажмите Calculate (Рассчитать).
3. Повторяйте шаг 1, используя другие параметры.



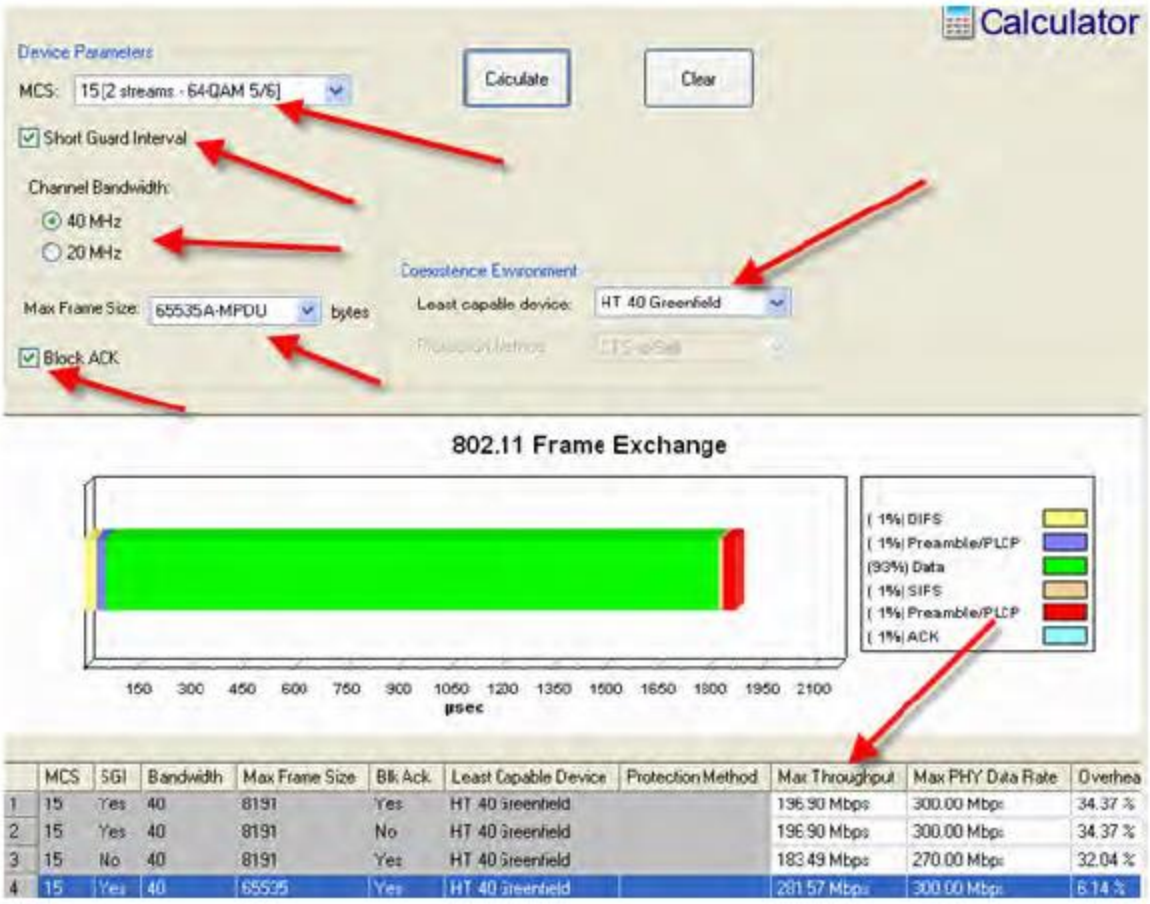
При каждом нажатии Calculate (Рассчитать) приложение AirMagnet WiFi Analyzer рассчитывает теоретический уровень пропускной способности, который можно ожидать от точки доступа, используя те же параметры. Это способно помочь установить реалистичные ожидания от новой развертываемой точки доступа, поскольку расчеты основаны на параметрах, которые указаны для нее пользователем. Калькулятор пропускной способности устройства также указывает объем служебных данных, необходимый для поддержки устаревших устройств.

Что следует учитывать при настройке новых точек доступа?

Перед настройкой новых точек доступа еще перед размещением их в сети можно убедиться, что все ключевые возможности 802.11n на точках доступа правильно настроены. На экране калькулятора пропускной способности устройства (Device Throughput Calculator) приложения AirMagnet WiFi Analyzer перечислены все важные параметры, которые необходимо учитывать при покупке или установке точек доступа.

Чтобы узнать о важных возможностях точек доступа 802.11n:

1. Откройте экран Device Throughput Calculator (Калькулятор пропускной способности устройства).
2. Просмотрите все параметры на экране Device Throughput Calculator, как показано на следующем рисунке.

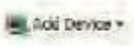


Все поля, выделенные на показанном выше рисунке, считаются очень важными для сетей 802.11n и должны приниматься во внимание при покупке или настройке точки доступа 802.11n. Они помогают принимать обоснованные решения для максимального увеличения пропускной способности ваших устройств или сетей 802.11n.

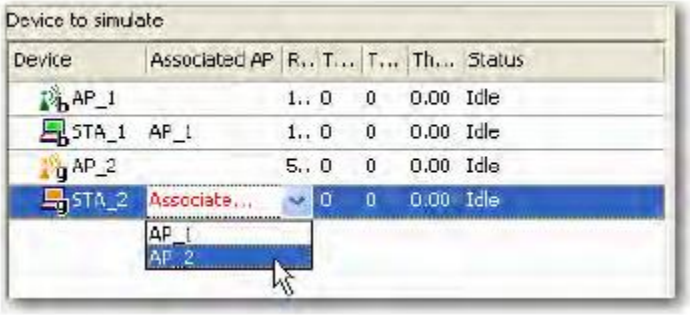
Какое изменение пропускной способности сети ожидается при развертывании новых точек доступа и/или станций в сети?

Пропускная способность сети, безусловно, будет зависеть от каждого добавленного нового устройства. Следовательно, может возникнуть необходимость моделирования радиочастотных условий при и после добавления в сеть различных устройств (точек доступа, станций и т.д.). Результаты моделирования заранее расскажут вам, чего следует придерживаться и/или чего следует избегать при установке новых точек доступа и станций. Всё это можно сделать прямо на экране инструмента Network Throughput Simulator (Моделирование пропускной способности сети) приложения AirMagnet WiFi Analyzer.

Для моделирования изменений в пропускной способности сети:

1. На экране WiFi Tools (Инструменты WiFi) щелкните кнопкой мыши на инструменте WLAN Throughput Simulator (Моделирование пропускной способности сети WLAN).
2. Выберите нужный диапазон частот, щелкнув кнопкой мыши на переключателе 2,4 ГГц или 5 ГГц.
3. На панели меню щелкните кнопкой мыши на 

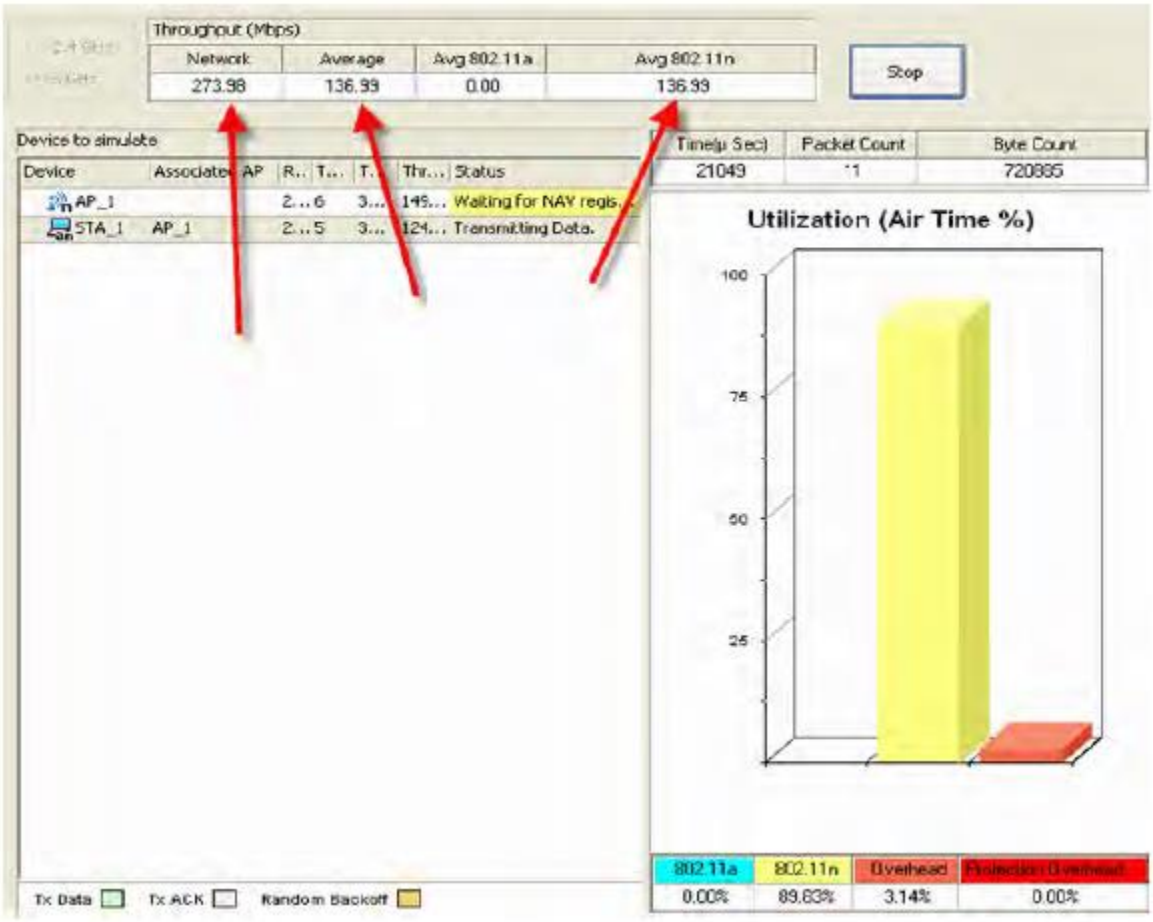
и выберите опцию в разворачивающемся меню.
4. Свяжите станцию с точкой доступа, щелкнув кнопкой мыши на станции, а затем на направленной вниз стрелке рядом с ней, чтобы выбрать нужную точку доступа, как показано на следующем рисунке.



5. Повторяйте шаг 3, чтобы связать все точки доступа и станции.

Примечание: Для запуска моделирования пропускной способности WLAN каждая станция должна быть связана с точкой доступа.

6. Нажмите кнопку Run (Выполнить) в правом верхнем углу экрана. Будет запущено моделирование, и его результаты будут отображаться на экране.



Функция моделирования пропускной способности сети (Network Throughput Simulator) позволяет моделировать пропускную способность WLAN при различных условиях, задаваемых пользователем. Это позволяет смоделировать воздействие на сеть, вызванное добавлением новых точек доступа и/или станций, связав станции с моделируемыми точками доступа или реальными точками доступа, уже

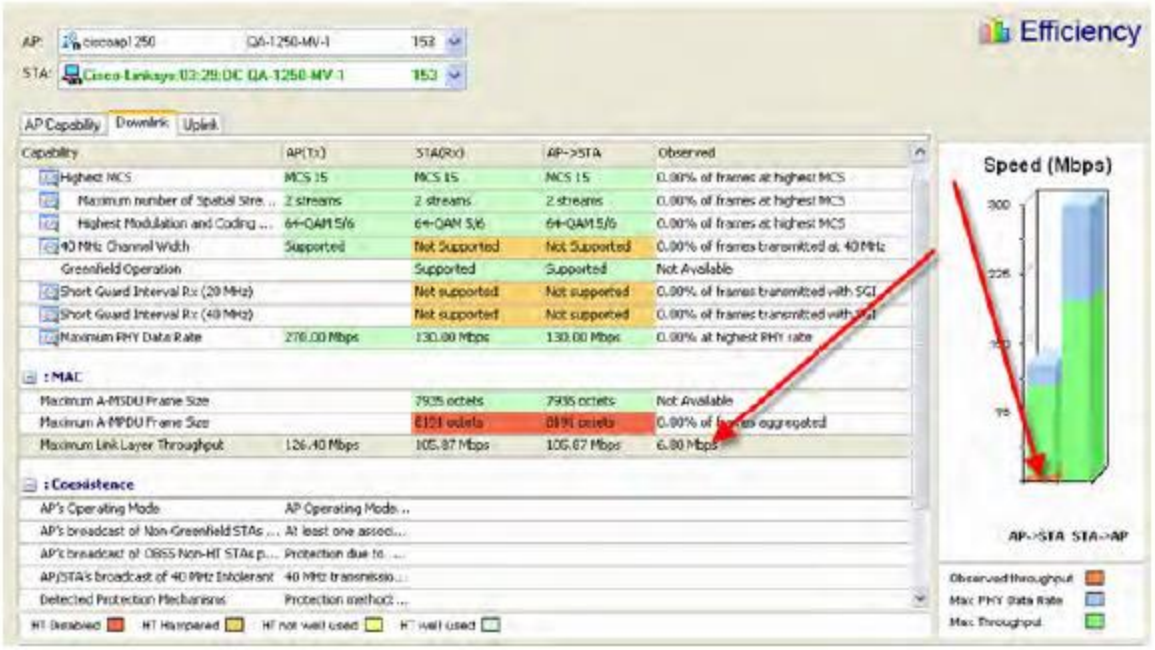
установленными на сети. Инструмент Simulator сформирует результаты и мгновенно отобразит их на экране.

Как узнать пропускную способность сети между точкой доступа и станцией?

Часто требуется узнать пропускную способность сети в реальном времени между определенной точкой доступа и определенной станцией. Инструмент Efficiency (Эффективность) приложения AirMagnet WiFi Analyzer делает эту информацию доступной, выводя ее на ваш рабочий стол.

Чтобы определить пропускную способность сети в реальном времени между точкой доступа и станцией:

1. Откройте экран WiFi Tools (Инструменты WiFi).
2. Щелкните кнопкой мыши на инструменте Efficiency (Эффективность).
3. Выберите нужную точку доступа и станцию.
4. Наблюдайте за данными в реальном времени на экране.



На экран Efficiency (Эффективность) выводятся исчерпывающие данные о пропускной способности между выбранной точкой доступа и станцией с точки зрения максимальной скорости передачи данных физического уровня (Max PHY Data Rate), максимальной пропускной способности канального уровня (Max Link Layer Throughput) и текущей скорости передачи данных (Current Data Rate). На экране показаны возможности точки доступа и статистика пропускной способности восходящего и нисходящего каналов при обмене данными между точкой доступа и станцией.

В столбцах Observed (Downlink) (Наблюдается (нисходящий канал)) и Observed (Uplink) (Наблюдается (восходящий канал)) на предыдущем рисунке в зависимости от ситуации может отображаться следующее:

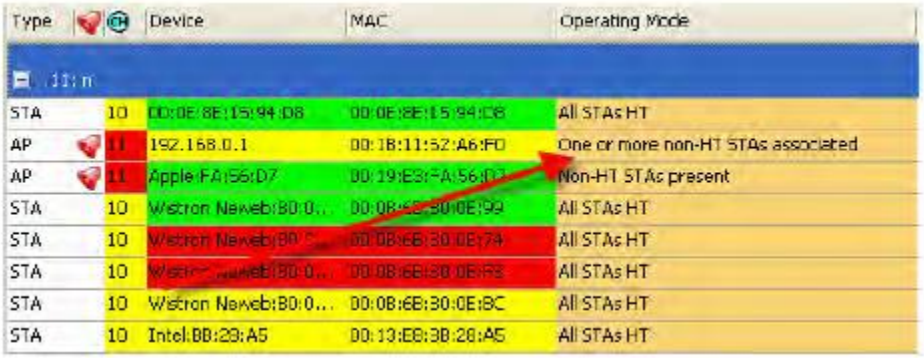
- Когда известно, что пара точка доступа – станция связана приложением AirMagnet WiFi Analyzer, столбец Observed содержит показания для конкретной связи точки доступа со станцией (то есть отображаются только измерения трафика, сделанные между комбинацией точки доступа и станции).
- Если известно, что пара точка доступа – станция не связана, столбец Observed содержит показания, которые не зависят от какой-либо связи (то есть отображаются все показатели исходящего трафика [данных] от точки доступа и станции).
- Когда выбрана точка доступа и «любая» станция, используются показания исходящего трафика (данных) точки доступа, а показания станции (то есть восходящей линии связи (Uplink)) равны нулю (трафик не указывается). В этом случае возможности точки доступа сравниваются с «виртуальной» станцией, параметры которой определены в нормах спецификации 802.11n.

Как узнать, связана ли моя точка доступа 802.11n с какими-либо устаревшими устройствами?

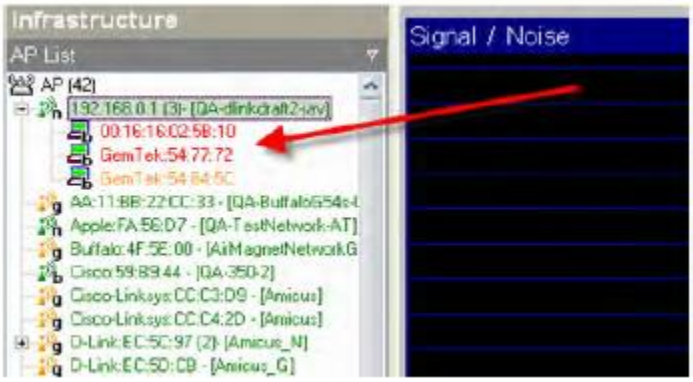
Несмотря на то, что точки доступа 802.11n имеют обратную совместимость с устаревшими устройствами, необходимо следить за тем, чтобы на точке доступа использовались механизмы защиты, которые позволят минимизировать или избежать потенциального негативного воздействия, которое сеть 802.11n оказывает на устаревшие устройства или сети. Для этого сетевые администраторы должны знать, связываются ли их точки доступа 802.11n с устаревшими устройствами. С помощью приложения AirMagnet WiFi Analyzer это можно сделать довольно легко.

Чтобы узнать, связываются ли ваши точки доступа 802.11n с устаревшими устройствами:

1. В приложении AirMagnet WiFi Analyzer выполните одно из следующих действий:
- Откройте экран Start, щелкните кнопкой мыши на Easy View (Простой просмотр) и выберите в разворачивающемся меню View by 802.11n (Просмотр по 802.11n).



- Откройте экран Infrastructure (Инфраструктура), щелкните кнопкой мыши на AP List (Список точек доступа) и разверните точку доступа 802.11n, с которой связаны станции.



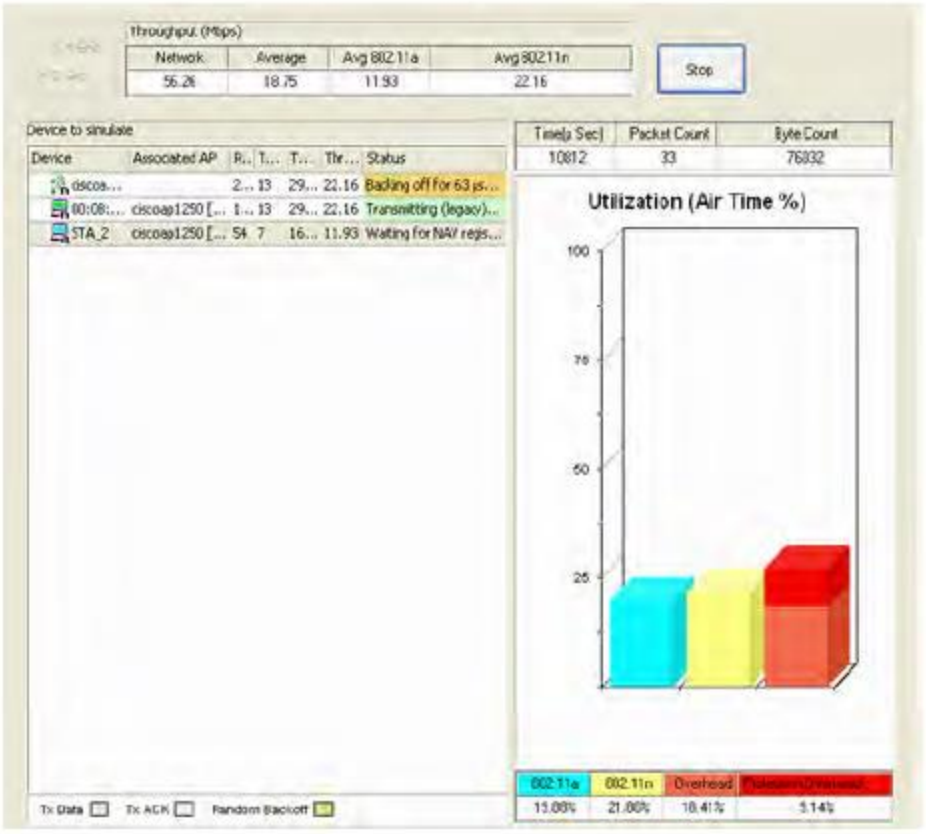
Сколько служебных данных использует точка доступа 802.11n для поддержки устаревших устройств?

Когда точки доступа 802.11n устанавливаются в непосредственной близости от устаревших сетей, то должны использовать защищенные служебные данные, чтобы минимизировать их влияние на устаревшие устройства. Функция моделирования пропускной способности сети (Network Throughput Simulator) позволяет легко определить процентную долю кадров, используемых для служебных данных точками доступа 802.11n в среде, где они сосуществуют с устаревшими устройствами.

Чтобы узнать служебные данные, используемые точкой доступа 802.11n:

1. Откройте экран WiFi Tool (Инструмент WiFi).

2. Щелкните кнопкой мыши на Network Throughput Simulator (Моделирование пропускной способности сети), выберите 2,4 ГГц или 5 ГГц и нажмите Run (Выполнить).



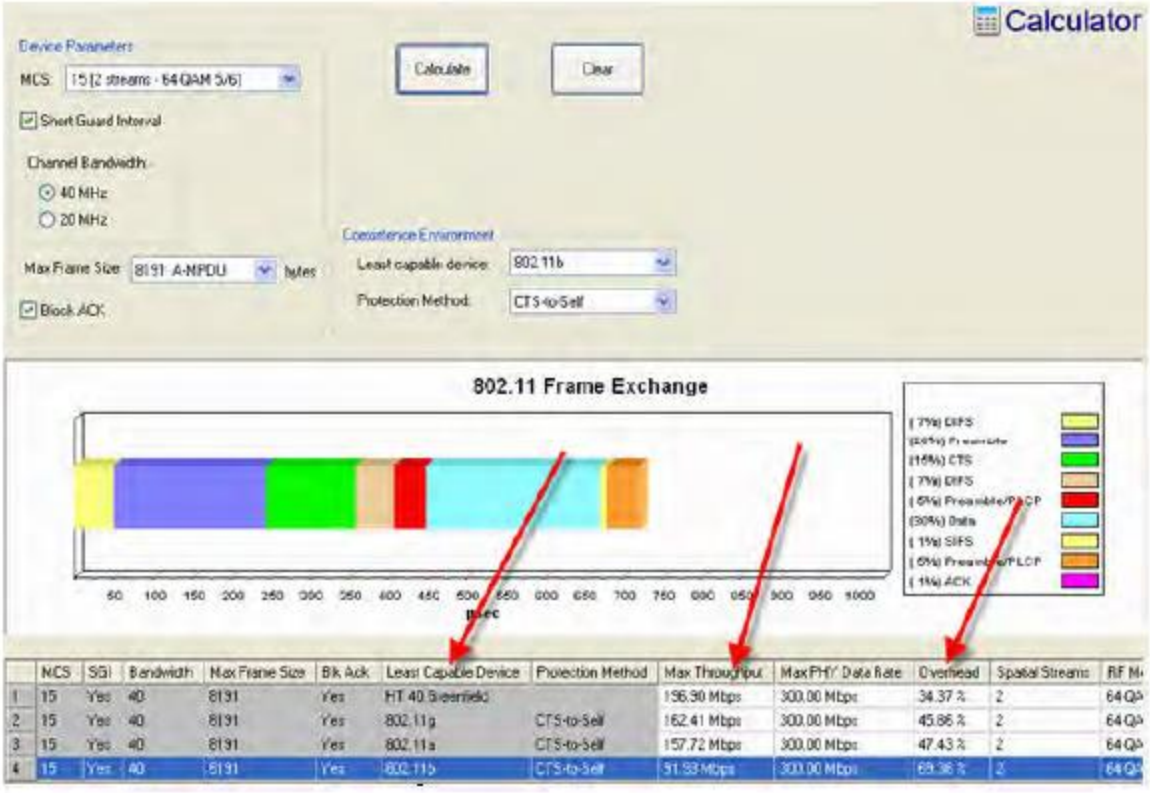
Функция Network Throughput Simulator позволяет моделировать пропускную способность сети WLAN в задаваемых пользователем условиях. Это обеспечивает визуализацию служебных данных, используемых точками доступа 802.11n для поддержания устаревших устройств, а также служебные данные, используемые для защиты передачи 802.11n от устаревших устройств.

Как связанные устаревшие устройства уменьшат пропускную способность устройства 802.11n?

Пропускная способность устройств 802.11n в присутствии устаревших устройств будет снижаться. Причина заключается в том, что устройства 802.11n должны использовать определенные механизмы защиты, чтобы защитить устаревшие устройства от потенциального вредного воздействия, которое передача 802.11n может оказывать на устаревшие устройства. Калькулятор пропускной способности устройства (Device Throughput Calculator) обеспечивает мгновенную обратную связь и позволяет узнать, как на пропускную способность устройства 802.11n повлияет использование различных менее производительных устройств.

Чтобы узнать, как связанные устаревшие устройства снижают пропускную способность устройства 802.11n:

1. Откройте экран Device Throughput Calculator (Калькулятор пропускной способности устройства).
2. Для наименее способного устройства (в среде сосуществования) (Least Capable Device) выберите 802.11b и выберите метод защиты (Protection Method).
3. Нажмите Calculate (Рассчитать).
4. Повторяйте шаги 2-3, чтобы рассчитать воздействие в различных условиях.



Экран инструмента Device Throughput Calculator (Калькулятор пропускной способности устройства) позволяет рассчитать пропускную способность устройства 802.11n с учетом наименее производительных устройств в сети. Также здесь показано увеличение служебных данных для приспособления к устаревшим устройствам.

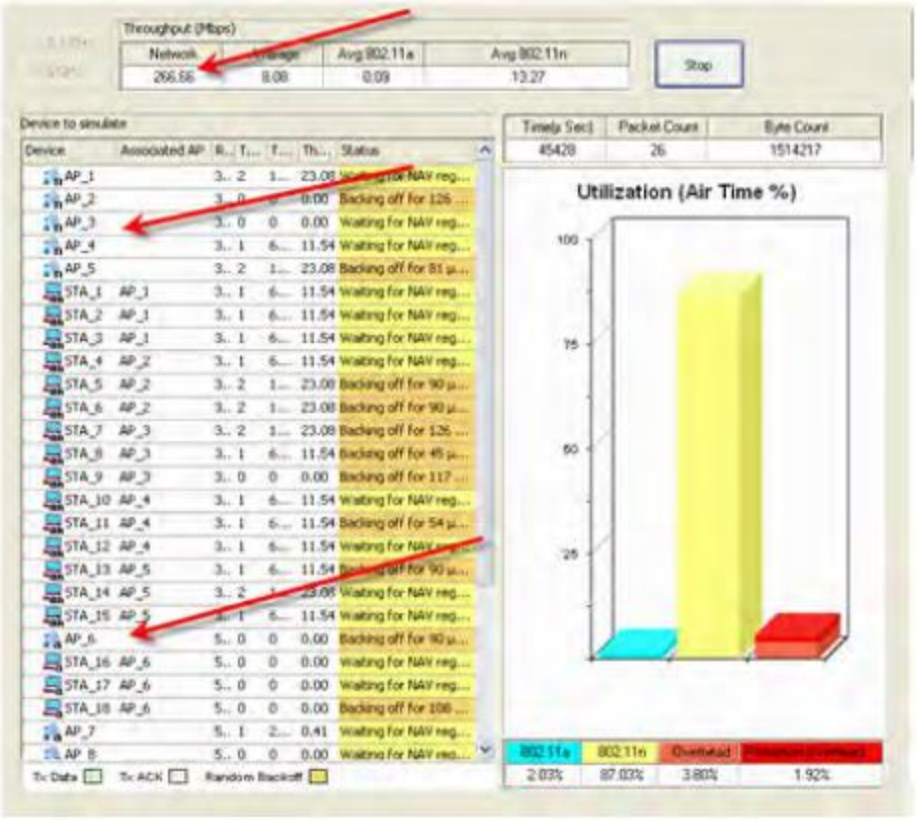
Сколько устаревших точек доступа можно добавить в сеть 802.11n?

Несмотря на то, что окончательная ратификация протокола 802.11n не за горами, реальность, с которой сталкиваются профессионалы в области беспроводных сетей, такова, что устаревшие сети и устройства не исчезнут в одночасье. Возможно, сети 802.11n и устаревшие устройства и сети будут сосуществовать долгие годы. Таким образом, сетевым специалистам обязательно нужно знать, сколько устаревших точек доступа можно добавить в сеть 802.11n, при этом поддерживая пропускную способность последней на определенном уровне. Эти данные можно легко получить с помощью инструмента Network Throughput Simulator (Моделирование пропускной способности сети) приложения AirMagnet WiFi Analyzer.

Чтобы узнать, сколько устаревших точек доступа можно добавить в сеть 802.11n:

1. Откройте экран инструмента Network Throughput Simulator (Моделирование пропускной способности сети).

2. Выберите 2,4 ГГц или 5 ГГц и нажмите Run (Выполнить).



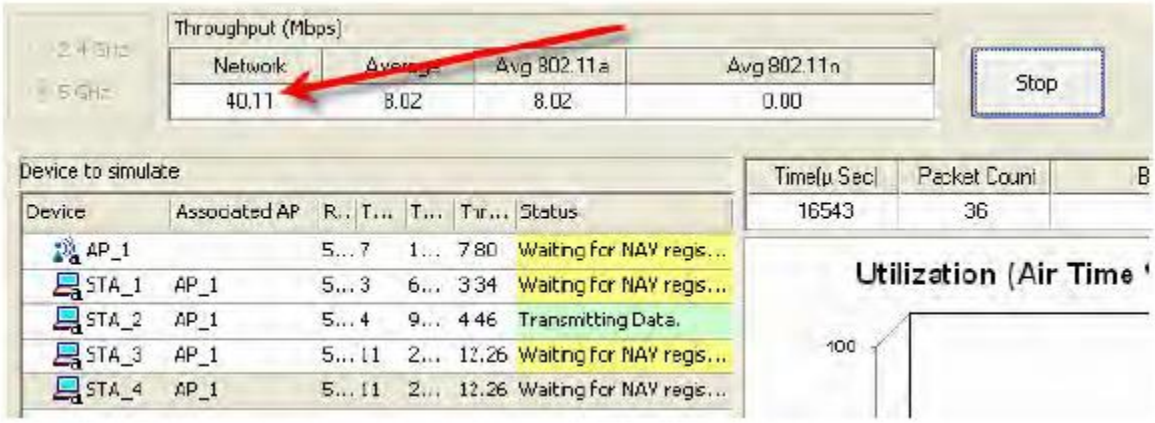
Инструмент Network Throughput Simulator (Моделирование пропускной способности сети) рассчитывает значения пропускной способности как на уровне узла, так и на уровне сети, полностью учитывая наименее производительные устройства в сети. Также инструмент моделирует влияние на сеть 802.11n добавления устаревших точек доступа, что можно легко визуализировать по мере добавления все большего количества устаревших устройств.

Как станции 802.11n влияют на существующую сеть 802.11a?

Когда станции стандарта 802.11n добавляются в сеть 802.11a, общая пропускная способность сети 802.11a повышается, поскольку оба эти стандарта поддерживают некоторые из новейших сетевых технологий 802.11. Это легко увидеть с помощью инструмента Network Throughput Simulator (Моделирование пропускной способности сети).

Чтобы определить положительное влияние станций 802.11n на существующую сеть 802.11g:

1. Откройте экран инструмента Network Throughput Simulator (Моделирование пропускной способности сети).
2. Выполните несколько моделирований, связывая станции 802.11a с сетью 802.11g, и обратите внимание на пропускную способность сети.



3. Выполните несколько моделирований, связывая станции 802.11a/n с той же сетью 802.11g, и обратите внимание на пропускную способность сети.

Как показано на рисунках выше, пропускная способность сети 802.11a составляла 40,11 Мбит/с при соединении со станциями 802.11a. Однако это значение увеличилось до 47,03 Мбит/с при соединении со станциями 802.11n. Это примерно на 17% больше.

Справочные материалы

Аббревиатуры и акронимы

В этом разделе перечислены аббревиатуры и акронимы, используемые в этом документе. Определения многих из этих терминов приведены в Глоссарии.

Аббревиатура или акроним	Полная форма	Перевод
ACK	Acknowledgement frame	Кадр подтверждения
ACL	Access Control List	Список контроля доступа
ACU	Cisco Aironet Client Utility	Утилита клиента Cisco Aironet
AES	Advanced Encryption Standard	Улучшенный стандарт шифрования
AirWISE	AirMagnet Wireless System Expert	Эксперт по беспроводной системе AirMagnet
AP	Access Point	Точка доступа
Auth.	Authentication	Аутентификация
BI	Beacon Interval	Сигнальный интервал
BSSID	Basic Service Set Identifier	Идентификатор основных наборов служб
CAD	Computer-Aided Design	Системы автоматизированного проектирования
CCI	Cross-Channel Interference	Межканальные помехи
CCKM	Cisco Centralized Key Management	Централизованное управление ключами Cisco
CF	Compact Flash	Флэш-карта (карта памяти)
CH	Channel	Канал
CRC	Cyclic Redundancy Check (Frame)	Циклический избыточный код (кадр)
Ctrl	Control (Frame)	Управление (кадр)
CTS	Clear to Send	Готовность к приему
dBm		дБм, децибелы относительно 1 милливатта
DCF	Distributed Coordination Function	Функция распределенной координации
DHCP	Dynamic Host Configuration Protocol	Протокол динамического конфигурирования хостов
Diag.	Diagnostics (Tool)	Диагностика (инструмент)
DNS	Domain Name System	Система доменных имен
DoS	Denial of Service	Отказ в обслуживании. Смотрите «DoS-атака»
DTIM	Delivery Traffic Indication Message	Сообщение с индикацией трафика доставки
EAP	Extensible Authentication Protocol	Протокол расширенной аутентификации
EAP-FAST	Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling	Протокол расширенной аутентификации - Гибкая аутентификация через безопасное туннелирование
EAP-TLS	Extensible Authentication Protocol with Transport Layer Security	Протокол расширенной аутентификации с безопасностью транспортного уровня
FCC	Federal Communications Commission	Федеральная комиссия связи
Frag.	Fragmentation	Фрагментация
GPS	Global Positioning System	Система глобального позиционирования
ICMP	Internet Control Message Protocol	Протокол управляющих сообщений Интернета
IEEE	Institute of Electrical and Electronics Engineering	Институт инженеров по электротехнике и радиоэлектронике
IP	Internet Protocol	Протокол Интернета
IPSec (VPN)	IP Security	IP-безопасность
IT	Information Technology	Информационные технологии
IV	Initialization Vector	Вектор инициализации
L2TP (VPN)	Layer 2 Tunneling Protocol	Протокол туннелирования уровня 2
LAN	Local Area Network	Локальная сеть
LEAP	Light EAP, Cisco LEAP	Легкий EAP, Cisco LEAP
MAC	Media Access Control	Управление доступом к среде
Mgmt	Management (Frame)	Менеджмент (кадр)
MIC	Message Integrity Code	Код целостности сообщения
PCF	Point Coordinated Function	Функция координации точек

PEAP	Protected Extensible Authentication Protocol	Защищенный протокол расширенной аутентификации
Perf.	Performance (Tool)	Функционирование (инструмент)
Ping	Packet Internet Grouper	Отправитель пакетов Интернет
PoE	Power over Ethernet	Питание через Ethernet
PPTP	Point-to-Point Tunneling Protocol	Протокол туннелирования точка-точка
RF	Radio Frequency	Радиочастота
RTS	Request to Send	Готовность к передаче
RTT	Round Trip Time	Время двукратного прохождения
S. Dist	Signal Distribution (Tool)	Распределение сигнала (инструмент)
S/N	Signal/Noise (ratio)	Сигнал-шум (соотношение)
SSID	Service Set Identity	Идентификатор набора служб
SSH (VPN)	Secure Shell Protocol	Протокол оболочки безопасности
STA	Station	Станция
STD	Standard Deviation	Стандартное (квадратическое) отклонение
TKIP	Temporal Key Integrity Protocol	Протокол ограниченной по времени целостности ключа
TLS	Transport Layer Security	Безопасность транспортного уровня
TTLS	Tunneled Transport Layer Security	Безопасность на туннельном транспортном уровне
Tx	Transmission	Передача
VoIP	Voice over IP	Голос по IP
VPN	Virtual Private Network	Виртуальная частная сеть
WAN	Wide Area Network	Глобальная сеть
WEP	Wired-Equivalent Privacy	Конфиденциальность, эквивалентная проводной сети
Wi-Fi	Wireless Fidelity	Беспроводная сеть
WLAN	Wireless Local Area Network	Беспроводная локальная сеть
WPA	Wi-Fi Protected Access	Защищенный доступ Wi-Fi

Глоссарий

802.11
Спецификация локальной сети IEEE, которая определяет канальный уровень доступа к беспроводной сети. Включает в себя подуровень управления доступом к среде передачи данных (MAC) 802.11 уровня канала передачи данных (Data Link Layer) и два подуровня физического (PHY) уровня - физический уровень FHSS (Расширение спектра со скачкообразной перестройкой частоты) и канальный уровень DSSS (Расширение спектра по методу прямой последовательности). Смотрите также 802.11a, 802.11b, 802.11e, 802.11g и 802.11i.

802.11a
Дополнение к спецификации беспроводной сети LAN (WLAN) IEEE 802.11, которая определяет передачу на физическом уровне (PHY) на основе ортогонального частотного разделения каналов (OFDM) в частотном диапазоне 5 ГГц и со скоростями передачи данных до 54 Мбит/с.

802.11ac
IEEE 802.11ac - это стандарт беспроводной компьютерной сети 802.11, обеспечивающий высокопроизводительную работу беспроводных локальных сетей в диапазоне 5 ГГц.
Теоретически эта спецификация обеспечит пропускную способность WLAN с несколькими станциями не менее 1 гигабит в секунду и максимальную пропускную способность одного канала не менее 500 мегабит в секунду (500 Мбит/с). Это достигается за счет расширения концепций радиоинтерфейса, использованной в стандарте 802.11n - более широкая радиочастотная полоса пропускания (до 160 МГц), больше пространственных потоков MIMO (до 8), многопользовательский MIMO и модуляция с высокой плотностью (до 256 QAM).

802.11b
Дополнение к спецификации WLAN IEEE 802.11, которое определяет передачу на физическом уровне (PHY) на основе DSSS (Расширение спектра по методу прямой последовательности) в частотном диапазоне 2,4 ГГц и со скоростями передачи данных до 11 Мбит/с.

802.11e
Дополнение к спецификации WLAN IEEE 802.11, которое определяет набор улучшений качества обслуживания (QoS) для приложений WLAN. Это позволяет отдавать более высокий приоритет аудио- и видеопотокам в реальном времени по сравнению с обычными данными. Этот стандарт считается критически важным для чувствительных к задержкам приложений, таких как передача голоса по беспроводному IP-протоколу (Voice over Wireless IP) и потоковая передача мультимедиа (Streaming Multimedia).

802.11g
Дополнение к спецификации WLAN IEEE 802.11, которая определяет передачу на физическом уровне (PHY) на основе OFDM (Ортогональное частотное разделение каналов) в частотном диапазоне 2,4 ГГц и со скоростями передачи данных до 54 Мбит/с.

802.11i
Стандартный протокол безопасности IEEE для беспроводной сети 802.11, который был разработан для замены исходного протокола WEP. Он обеспечивает сложную аутентификацию с использованием различных протоколов (например, 802.11x, EAP и RADIUS) и надежную защиту с помощью протокола шифрования AES-CCMP. Также известен как WPA2.

802.11n
IEEE 802.11n-2009 является поправкой к стандарту беспроводной сети IEEE 802.11-2007, которая обеспечивает значительное увеличение максимальной скорости передачи полезных данных с 54 Мбит/с до 600 Мбит/с за счет использования четырех пространственных потоков при ширине канала 40 МГц. [1] [2] Стандартизованная поддержка 802.11n для систем с множеством входов/множеством выходов и агрегированием кадров, а также, помимо прочего, улучшением безопасности.

802.11X
Первичный стандарт IEEE 802.11 для управления доступом к сети на основе портов. Базирующийся на протоколе расширенной аутентификации (Extensible Authentication Protocol - EAP) стандарт 802.11X предоставляет структуру аутентификации, которая поддерживает различные методы аутентификации и авторизации доступа к сети как для проводных, так и для беспроводных пользователей.

Список контроля доступа (ACL)
Список известных беспроводных устройств, хранящийся в сетевом маршрутизаторе или коммутаторе и используемый для управления доступом к сети и из нее.

Подтверждение (ACK)
Согласно протоколу TCP/IP, пакеты ACK используются для подтверждения получения пакетов. Пакеты ACK широко используются в сетях 802.11 для обеспечения надежной передачи данных в ненадежной среде.

Усовершенствованный стандарт шифрования (AES)
Являясь одним из федеральных стандартов обработки информации (FIPS), стандарт AES определяет алгоритм симметричного шифрования для защиты конфиденциальной информации, передаваемой по общедоступным сетям. Смотрите Публикацию 197 FIPS.

Режим Ad Hoc
Режим беспроводной сети, при котором подключенные к беспроводной сети устройства могут напрямую взаимодействовать друг с другом без использования точки доступа или проводной сети. Также известен как одноранговый режим или набор основных независимых служб (IBSS).

Точка доступа (AP)
Аппаратное устройство, которое связывает или соединяет беспроводные станции с проводной сетью. Точки доступа используются для централизации всех беспроводных станций в локальной сети в так называемом «инфраструктурном» режиме. Обычно они используются в больших офисных зданиях или таких общественных местах, как аэропорты, для формирования одной беспроводной локальной сети (WLAN), охватывающей большую территорию. Каждая точка доступа обычно поддерживает 255 беспроводных станций. Также известна как точка беспроводного доступа или WAP.

Эксперт по беспроводным системам AirMagnet (AirWISE)
Запатентованный AirMagnet инструмент анализа беспроводных сетей, который в режиме реального времени автоматически уведомляет ИТ-специалистов и сетевых специалистов о состоянии WLAN, включая безопасность, производительность и конфигурацию сети, а также предоставляет контекстно-зависимый анализ и рекомендации для конкретных случаев.

Соединение
Взаимоотношения или связь, установленная между беспроводной станцией (например, портативным компьютером) и беспроводной точкой доступа, по которой станция получает услуги от точки доступа.

Аутентификация
Любая мера безопасности, принятая для установления действительности передачи, сообщения или отправителя, или процесс проверки разрешения определенной стороне получать определенную информацию.

Полоса пропускания
В компьютерных сетях - скорость передачи данных, поддерживаемая сетевым соединением или интерфейсом. Полоса пропускания представляет собой общие возможности соединения. Чем больше полоса пропускания, тем выше производительность, хотя на общую производительность сети также могут влиять такие факторы, как задержка, использование и т.д.

Маяк
В беспроводной сети - пакет, отправляемый одним сетевым устройством другим сетевым устройствам и информирующий их о своем присутствии и готовности.

Сигнальный интервал
Продолжительность времени ожидания передающего устройства перед повторной отправкой сигнала маяка. При отправке сигнала маяка устройство, подключенное к беспроводной сети, будет включать в него интервал маяка, который сообщает подключенным к сети принимающим устройствам, как долго они могут ждать в режиме пониженного энергопотребления, прежде чем проснутся для обработки сигнала маяка. Сигнальный интервал обычно измеряется в миллисекундах (мс).

Мостовой режим
В беспроводной сети режим моста позволяет двум WAP (точкам беспроводного доступа) связываться друг с другом для объединения нескольких локальных сетей. В то время как некоторые беспроводные мосты поддерживают только одно соединение «точка – точка» с другой точкой доступа, другие поддерживают многоточечные соединения (точка – многоточка) с несколькими точками доступа. Возможность использования моста (если доступна) может быть включена или отключена на точке доступа с помощью параметра настройки конфигурации. При работе в режиме моста беспроводные точки доступа потребляют значительную часть полосы пропускания. Беспроводные станции в мостовой сети 802.11 обычно используют ту же полосу пропускания, что и мостовые устройства. Поэтому они, как правило, работают медленнее.

Рассылка
Процесс отправки одних и тех же данных на все станции в сети. Смотрите многоадресную и одноадресную рассылку.

Идентификатор основных наборов служб (BSSID)
Уникальный идентификатор точки доступа в сети с основным набором служб (BSS). Это 48-битный MAC-адрес радиомодуля внутри точки доступа, который обслуживает станции в сети BSS.

Канал
Радиочастота или полоса частот, присвоенная определенной стране или региону мира международным соглашением. Например, 802.11b состоит из 14 нелицензируемых каналов (то есть каналов 1–14) в диапазоне 2,4 ГГц (то есть от 2412 МГц до 2484 МГц с шагом 5 МГц).

Централизованное управление ключами Cisco (CCKM)
Схема управления ключами шифрования, определенная компанией Cisco, которая позволяет беспроводным устройствам быстро и безопасно перемещаться в домене управления WLAN. CCKM включает защиту от распространенных векторов атак, таких как спуфинг, атака путем повтора перехваченных данных или атаки типа «злоумышленник посередине». Работает при наличии 802.1x со схемой аутентификации EAP при условии, что клиентское устройство ее поддерживает.

CiscoWorks Wireless LAN Solution Engine (WLSE)
Важный компонент инфраструктуры Cisco SWAN, который предоставляет возможности для управления WLAN, включая внесение изменений в конфигурацию, создание отчетов, сбор информации о радиомониторинге и управлении, а также выполнение обнаружения устройств.

Готовность к приему (CTS)
Сигнал RS-232, отправляемый от принимающей станции к передающей станции и указывающий, что она готова принять данные.

Помехи в совмещенном канале
Термин, который относится к помехам от двух или более точек доступа, работающих на одном радиоканале.

Флэш-карта (CF)
Тип флеш-памяти. Компактные флэш-карты обычно используются в цифровых камерах для хранения изображений, но также применяются и в карманных компьютерах и музыкальных проигрывателях. Существует два типа CF-карт: Тип I и Тип II. Первый имеет толщину 3,3 мм, а второй - 5 мм.

Компьютерное проектирование (САПР)
Чертеж, создаваемый с помощью программного приложения, которое помогает в точном рисовании. Приложения САПР широко используются в художественных, архитектурных, инженерных и производственных применениях.

Авария
Любой критический сбой в компьютере, сетевом устройстве или программном приложении, которое работает на таких устройствах. Когда происходит авария, компьютер может зависнуть на неопределенное время. Авария может произойти без предупреждения. Для восстановления после подобной аварии пользователю может потребоваться выключить питание, а затем перезагрузить компьютер или сетевое устройство.

Циклическая проверка четности с избыточностью (CRC)
Метод проверки ошибок, используемый для обеспечения точности передаваемых по сети данных. Каждое переданное сообщение разбивается на заранее определенные отрезки, которые затем делятся на фиксированный делитель. Остальная часть вычислений добавляется и отправляется вместе с сообщением. После получения сообщения принимающая станция пересчитывает остаток. Ошибка обнаруживается, когда она не совпадает с переданным остатком.

Функция распределенной координации (DCF)
Метод управления доступом к среде (MAC), используемый для управления передачей данных по среде в сети WLAN. Позволяет беспроводному узлу прослушивать окружающие его узлы, чтобы определить, передают ли они, прежде чем передавать самому. Смотрите PCF.

Стандарт шифрования данных (DES)
Метод шифрования, первоначально разработанный IBM и сертифицированный правительством США для передачи несекретных данных. Использует алгоритм шифрования с частным ключом, согласно которому отправитель и получатель используют один и тот же частный ключ. Ключ состоит из 56 бит данных, которые преобразуются и комбинируются с каждым 64-битным отправляемым блоком данных.

Целостность данных
Достоверность данных, передаваемых по сети. Обеспечение достоверности требует принятия мер, гарантирующих, что содержимое данных не будет искажено и изменено. Наиболее распространенный метод – использование односторонней хеш-функции (функции расстановки ключей), которая объединяет все байты в сообщении с секретным ключом и создает дайджест сообщения, который невозможно отменить. Проверка целостности – ключевой компонент обеспечения безопасности данных.

дБм (децибелы относительно милливатта)
В беспроводной сети мощность передачи или приема устройства измеряется в децибелах относительно мощности в один милливатт. Чем выше значение дБм, тем выше мощность передачи или приема устройства.

Сообщение с индикацией трафика доставки (DTIM)
Сигнал, передаваемый точкой доступа как часть маяка на станцию в режиме энергосбережения, предупреждающий устройство о том, что пакет ожидает доставки.

Система доменных имен (DNS)
Система разрешения имен и адресов, которая автоматически преобразует имена доменов и хостов в Интернете в IP-адреса. DNS устраняет необходимость ручного обновления файлов хостов в сети. Также известна как служба доменных имен (Domain Name Service), сервер доменных имен (Domain Name Server).

Протокол динамической конфигурации хоста (DHCP)
Программное приложение, которое автоматически назначает IP-адреса станциям, входящим в сеть TCP/IP. Программное обеспечение DHCP обычно работает на сетевых серверах, а также на сетевых устройствах, например, маршрутизаторах ISDN, маршрутизаторах модемов и т.д., которые позволяют множеству пользователей получать доступ в сеть Интернет. DHCP избавляет сетевых специалистов от необходимости вручную назначать IP-адреса.

Шифрование
Обратимое преобразование данных из исходного вида в формат, который трудно интерпретировать (зашифрованный), используемое как способ защиты их конфиденциальности, целостности, а иногда и подлинности. Предполагает использование алгоритма шифрования и одного или нескольких ключей шифрования.

Ethernet
Стандарт, используемый для соединения компьютеров в локальную сеть (LAN).

Протокол расширенной аутентификации (EAP)
Протокол, который используется в качестве основы и транспорта для других протоколов аутентификации. EAP использует свои собственные начальные и конечные сообщения, но также может передавать любое количество сторонних сообщений между станцией и точкой доступа в беспроводной сети.

Протокол расширенной аутентификации - Гибкая аутентификация через безопасное туннелирование (EAP-FAST)
Усовершенствование протокола LEAP от Cisco, которое предоставляет зашифрованный туннель для передачи заранее установленных ключей совместного использования, известных как ключи с кодом персональной аутентификации (PAC). Для предотвращения словарных атак ключи PAC могут постоянно обновляться. EAP-FAST обеспечивает безопасный доступ к беспроводной сети.

Протокол расширенной аутентификации - безопасность транспортного уровня (EAP-TLS)
Протокол безопасности беспроводной сети, созданный Microsoft и принятый IETF. Смотрите «RFC 2716: PPP EAP TLS Authentication Protocol».

Протокол расширенной аутентификации - безопасность туннельного транспортного уровня (EAP-TTLS)
Собственный протокол, разработанный Funk Software и Certicom и поддерживаемый Agere Systems, Proxim и Avaya. IETF рассматривает его как новый стандарт для беспроводных сетей.

Федеральная комиссия связи (FCC)
Агентство федерального правительства США, регулирующее связь в стране.

Кадр
В системах связи – фиксированный блок данных, передаваемый по сети как единое целое.

FTP
Стандартный сетевой протокол, используемый для копирования файла с одного хоста на другой по сети на основе протоколов TCP/IP, в частности, сети Интернет.

Глобальная система позиционирования (GPS)
Спутниковая радионавигационная система, эксплуатируемая Министерством обороны США. Используется для определения местоположения на планете. Путем триангуляции сигналов от трех спутников приемное устройство может определить свое местоположение в любой точке Земли с точностью до 20 метров по горизонтали.

Точка беспроводного публичного доступа
В беспроводной сети - определенное место в зоне действия точки доступа, где широкая публика может использовать сетевую услугу, как правило, за определенную плату.

HTTP
Сетевой протокол для распространения данных в сети Интернет (World Wide Web).

Инфраструктурный режим
Настройка беспроводной сети, в которой все станции связываются с сетью или друг с другом через точку доступа. Инфраструктурный режим типичен для корпоративной беспроводной сети.

Институт инженеров по электротехнике и радиоэлектронике (IEEE)
Некоммерческая инженерная организация в США, которая разрабатывает, пересматривает и продвигает стандарты в электронной и компьютерной промышленности.

Помехи
В беспроводной сети - помехи, возникающие при столкновении в эфире радиосигналов от разных точек доступа.

IP-адрес
32-битная уникальная последовательность цифровых символов, используемая для идентификации сетевого компьютера, принтера или любого другого устройства.

Джиттер
Колебания радиосигнала, наблюдаемые в трафике между точкой доступа и станцией в беспроводной сети.

Облегченный протокол расширенной аутентификации (LEAP)
Собственный протокол для безопасного доступа к сети WLAN, разработанный компанией Cisco.

Локальная сеть (LAN)
Сеть ближнего действия, объединяющая группу компьютеров, обычно в одном здании. Используя сетевой концентратор в качестве точки подключения, по сети можно отправлять данные с одного компьютера на другой.

Среда
В беспроводной сети этот термин относится к типам среды 802.11, используемой в беспроводных сетевых устройствах, то есть 802.11a, 802.11b и 802.11g.

Адрес управления доступом к среде (MAC-адрес)
Уникальный 48-битный номер, назначаемый каждому сетевому IP-адаптеру. Он записывается в виде последовательности из 12 шестнадцатеричных цифр (например, 46:2F:0B:19:11:CB). Каждый MAC-адрес уникален и устанавливается производителем сетевого устройства; иногда он называется «физическим адресом» устройства. Первые шесть шестнадцатеричных цифр MAC-адреса соответствуют уникальному идентификатору производителя, а последние шесть цифр соответствуют серийному номеру устройства.

Многоадресная рассылка
Процесс отправки одного сообщения нескольким адресатам одновременно. Это передача «один ко многим» похожа на широковещательную рассылку, за исключением того, что многоадресная передача означает передачу определенным группам, тогда как широковещательная передача подразумевает отправку всем. Многоадресная рассылка способна значительно сэкономить полосу пропускания при отправке больших объемов данных, поскольку основная часть данных передается один раз от источника по основным магистралям и распределяется в точках переключения, расположенных ближе к получателям. В одноадресной системе данные полностью копируются для каждого получателя. Сравните с одноадресной рассылкой.

Сетевой адаптер
Аппаратное устройство, которое связывает станцию (например, компьютер) с сетью. Современные аппаратные сетевые адаптеры могут иметь разную форму, например, в виде карт PCI Ethernet, устройств PCMCIA или USB-устройств. Некоторые портативные компьютеры даже поставляются со встроенными адаптерами беспроводной сети, предварительно установленными на них в виде микросхем. Операционные системы поддерживают сетевые адаптеры с помощью программного обеспечения, известного как «драйвер устройства», которое позволяет прикладному программному обеспечению взаимодействовать с адаптером. Некоторые сетевые адаптеры представляют собой программные пакеты, имитирующие работу сетевого адаптера. Также такие адаптеры известны как беспроводная сетевая карта, карта Wi-Fi.

Шум
В беспроводной сети - любой радиосигнал, не несущий полезной информации. Смотрите также отношение сигнал-шум (S/N или SNR).

Ping
В беспроводной сети - приложение, которое используется для отправки пакета через Интернет для проверки подключения удаленного узла. Если пакет возвращается, это означает, что удаленное устройство подключено.

Функция координации точек (PCF)
Используемая в сетях WLAN технология управления доступом к среде (MAC), в которой для связи с другим узлом беспроводной узел полагается на точку доступа как на центральный узел. Прежде чем разрешить узлу передачу, точка доступа слушает, чтобы убедиться, что эфир свободен (то есть, нет никакого другого трафика данных).

Защищенный протокол расширенной аутентификации (PEAP)
Протокол, совместно разработанный Microsoft, Cisco и RSA Security.

Готовность к передаче (RTS)
Сообщение, отправляемое сетевой станцией на соответствующую точку доступа или станцию с запросом разрешения на передачу данных.

Роуминг
В беспроводной сети - способность беспроводного устройства (станции) поддерживать сетевое соединение при перемещении между разными сотами (ячейками) сети, обслуживаемыми разными точками доступа.

Идентификатор набора служб (SSID)
Уникальное имя, идентифицирующее беспроводную сеть или ее подмножество. Используется каждым устройством, подключенным к сети или части сети, для идентификации себя как части семейства при получении доступа к сети или проверке происхождения передаваемого пакета данных.

Сигнал
В беспроводной сети - любой электрический импульс или частота, передающая значимые данные в эфире.

Отношение сигнал-шум (S/N или SNR)
Отношение амплитуды сигнала к амплитуде смешивающегося с ним фонового шума (помех), измеряемое в децибелах. Определяет чистоту сигнала в канале беспроводной передачи. Чем выше значение, тем меньше шумов и тем выше качество сигнала. Отношение сигнал/шум 0 (ноль) означает, что уровни шума и сигнала одинаковы, что является самым низким значением, которое только может быть.

Станция (STA)
В беспроводной сети любое устройство с MAC-адресом и интерфейсом физического уровня (PHY) для подключения к беспроводной среде, которое соответствует стандарту IEEE 802.11, например ноутбук, КПК и т.д.

Протокол ограниченной по времени целостности ключа (TKIP)
Протокол безопасности, определенный в спецификациях IEEE 802.11i для сетей WLAN. Был разработан для замены протокола WEP без замены устаревшего оборудования. Подобно протоколу WEP, протокол TKIP использует схему ключей, основанную на RC4, за исключением того, что он шифрует каждый передаваемый пакет данных, используя свой собственный уникальный ключ шифрования. Протокол TKIP также хэширует значения IV (Вектор инициализации), которые передаются в текущей версии WEP, а это означает, что IV также зашифрованы, и их не так легко перехватить в эфире.
TKIP обеспечивает смешивание ключей для каждого пакета, проверку целостности сообщения и механизм смены ключей, тем самым решая другие проблемы безопасности с WEP. Это увеличивает сложность декодирования ключей за счет уменьшения количества доступных взломщику данных, которые были зашифрованы с использованием определенного ключа.
Протокол беспроводного шифрования, который устраняет известные лазейки безопасности в протоколе WEP для существующих устройств 802.11b. Протокол TKIP поставляется с 128-битным ключом шифрования, 48-битным вектором инициализации (IV), кодом целостности сообщения (MIC) и правилами упорядочения вектора инициализации, что позволяет обеспечить лучшую защиту, чем WEP.

Traceroute (отслеживание маршрута)
Утилита IP-сети, которая используется для определения пути от передающей станции к удаленному узлу, с которым осуществляется связь, в режиме реального времени. Позволяет обнаружить IP-адреса всех маршрутизаторов между ними.

Безопасность транспортного уровня (TLS)
Протокол аутентификации и шифрования для частной передачи через Интернет. Обеспечивает взаимную аутентификацию с предотвращением отказа, шифрованием, согласованием алгоритмов, безопасным получением ключей и проверкой целостности сообщений. Являясь преемником протокола Secure Socket Layer (SSL), протокол TLS был адаптирован для использования в сетях WLAN и широко используется в аутентификации IEEE 802.11x.

Безопасность на туннельном транспортном уровне (TTLS)
Подпротокол EAP (Extensible Authentication Protocol), разработанный Funk Software, Inc. для аутентификации 802.11x. Использует в качестве средства аутентификации запрос и ответ комбинации сертификатов и пароля. TTLS поддерживает методы аутентификации, определенные EAP, а также более старый протокол CHAP (Challenge Handshake Authentication Protocol – Протокол аутентификации при установлении вызова), PAP (Password Authentication Protocol - Протокол аутентификации по паролю), Microsoft CHAP (MS-CHAP) и MS-CHAPV2.

Одноадресная рассылка
Процесс отправки дубликатов одного и того же сообщения нескольким адресатам в сети. При одноадресной передаче, даже если несколько пользователей могут запрашивать одни и те же данные с одного и того же сервера в одно и то же время, передаются повторяющиеся потоки данных, по одному каждому адресату. Сравните с многоадресной рассылкой.

Передача голоса по IP (VoIP)
Технология, используемая для передачи телефонных голосовых сигналов в виде IP-пакетов через Интернет или выделенную IP-сеть в соответствии со спецификацией Сектора стандартизации Международного союза электросвязи (ITU-T) H.323. Это позволяет маршрутизатору передавать телефонные звонки и факсы через Интернет без потери функциональности, надежности или качества голоса. Также известна как IP-телефония или Интернет-телефония.

Конфиденциальность, эквивалентная проводной сети (WEP)
Протокол безопасности в рамках стандарта IEEE 802.11, который обеспечивает беспроводную локальную сеть WLAN с минимальным уровнем безопасности и конфиденциальности, сопоставимым с типичной проводной локальной сетью. Протокол WEP шифрует данные, передаваемые по WLAN, для защиты уязвимого соединения между точками доступа и станциями. Однако, поскольку WEP регулирует доступ к WLAN на основе MAC-адреса устройства, который относительно легко перехватить и украсть, он обеспечивает ограниченную безопасность для WLAN.

Беспроводная локальная сеть (WLAN)
Локальная сеть (LAN), к которой беспроводные пользователи (станции) могут подключаться и общаться с помощью высокочастотных радиосигналов, а не медных проводов.

Защищенный доступ Wi-Fi (WPA)
Протокол безопасности для стандарта IEEE 802.11, предназначенный для преодоления уязвимостей безопасности WEP. Технология предназначена для работы с существующими беспроводными устройствами, поддерживающими протокол WEP, но предлагает два важных улучшения по сравнению с WEP: улучшенное шифрование данных с помощью TKIP и аутентификацию пользователя с помощью EAP. Протокол TKIP предназначен только для подмножества протокола IEEE 802.11i и разработан для работы в более старых устройствах с поддержкой WEP путем обновления их микропрограмм до WPA.
С другой стороны, протокол WPA2 предлагает полную поддержку стандарта 802.11i. Помимо TKIP, он поддерживает протокол шифрования AES-CCMP, который основан на очень безопасном национальном стандартном шифре AES, объединенном со сложными методами шифрования, и специально разработан для сетей WLAN.

Лицензия и авторские права

ОБЩИЕ ПОЛОЖЕНИЯ И УСЛОВИЯ

(версия на 01 октября 2019 года)

Настоящие Общие положения и условия заключаются между юридическими лицами, указанными в соответствующем Заказе («Компания»), дополнительно определенном ниже, и устанавливают условия, права и ограничения, в отношении которых LinkRunner, LLC d/b/a NetAlly и любые ее дочерние компании и аффилированные лица (вместе или по отдельности именуемые «NetAlly») готовы продавать устройства («Оборудование») и лицензировать проприетарное программное обеспечение NetAlly, а также любую прошивку, находящуюся на таком Аппаратном обеспечении («Программное обеспечение») (Аппаратное обеспечение и программное обеспечение могут совместно именоваться «Продукт (-ы)») и предоставлять Компании услуги по обслуживанию и технической поддержке («Обслуживание»). Если иное не предусмотрено подписанным контрактом между Компанией и NetAlly, к любым Заказам, сделанным в отношении Продуктов NetAlly, будут применяться только настоящие Общие условия и положения. Предоставление компанией NetAlly Продуктов, Обслуживания или любых других услуг прямо зависит от принятия Компанией настоящих Общих условий и положений «КАК ЕСТЬ».

Получение Компанией каких-либо Продуктов от NetAlly без возврата считается принятием этого Заказа, а также является подтверждением Компании того, что описания Продуктов, их количество, срок и цены, указанные в Заказе, точно отражают предполагаемую Компанией покупку. Все дополнительные и противоречащие положения и условия, представленные с любым или в любом сообщении, включая, помимо прочего, изложенные в любой заявке на приобретение, за исключением цены, количества и местоположения, настоящим отклоняются и считаются недействительными.

1. Определения.

«API» означает интерфейсы программных приложений и рабочие процессы, которые компания NetAlly делает общедоступными в определенных Продуктах для обеспечения интеграции, реализации и взаимодействия с оборудованием и программным обеспечением третьих сторон.
«Компания» означает действующее юридическое лицо с хорошей репутацией, которое заключило коммерческое соглашение с NetAlly, разрешающее лицензирование или повторное лицензирование Программного обеспечения, а также распространение, продажу или перепродажу Продуктов и Услуг.
«Данные компании» означает информацию, которую Компания выгружает или использует в связи с использованием этой Компанией Продуктов.
«Закон о защите данных» означает Закон о переносимости и подотчетности медицинской информации (HIPAA) (29 Свод законов США, § 1181 и последующие), Закон Грэмма Лича Блайли (GLBA) (15 Свод законов США, § 1681), Общие правила защиты данных (GDPR). (EU 2016/679) и другие применимые правила, направленные на защиту обработки и хранения личной информации.
«Документация» означает любые руководства по установке, справочные руководства, руководства по эксплуатации и примечания к выпуску, поставляемые с Продуктом в печатной, электронной или онлайн-форме.
«Пробный продукт» означает программное обеспечение, которое содержит лицензионный ключ, отключающий Программное обеспечение через 30 дней или другой срок, согласованный сторонами, и который делает Продукт непригодным для использования.
«Заказ» означает комбинацию сделанной Компанией заявки на приобретение, сделанного NetAlly или ее дочерними компаниями Ценового предложения и настоящих Общих условий и положений.
«Персональные данные» означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу (далее «Субъект данных»); идентифицируемое лицо - это лицо, которое может быть идентифицировано прямо или косвенно, в частности, по идентификационному номеру или одному или нескольким факторам, характерным для его физической, физиологической, умственной, экономической, культурной или социальной идентичности.
«Р.О.» означает заявку на приобретение или документ в материальной или нематериальной форме (например, форматах .rtf, .pdf и т.д.), выпущенный Компанией, свидетельствующий о принятии Компанией Ценового предложения и настоящих Общих условий и положений, без учета каких-либо противоречащих друг другу положений и условий, представленных в них, за исключением цены, количества и местонахождения Продуктов или Услуг.
«Ценовое предложение» означает документ, в соответствии с которым NetAlly предлагает к продаже и лицензирует свои Продукты, Обслуживание и другие услуги.
«Услуги» означают Обслуживание, а также любые другие услуги, которые NetAlly время от времени предлагает Компании.

2. Условия отгрузки и доставки. NetAlly отправляет все Продукты на условиях FOB Origin. Если стороны не договорились об ином, все перевозки будут осуществляться с использованием перевозчика, указанного Компанией. Если Компания не назначает перевозчика, NetAlly оставляет за собой право выбрать его за счет Компании. Для Программного обеспечения, доступного для электронной загрузки, доставка будет считаться осуществленной после того, как NetAlly сделает Программное обеспечение доступным для загрузки Компанией или ее уполномоченным агентом или представителем. Если иное не указано явно на лицевой стороне применимого Заказа, NetAlly оставляет за собой право выполнять Заказы с помощью нескольких отправлений. Для всей Продукции, поставляемой за границу, Компания будет являться зарегистрированным импортером. Компания соглашается с тем, что не будет удалять какие-либо Общие положения и условия NetAlly или другие соглашения из Продуктов NetAlly и/или связанной с ними упаковки.

3. Предоставление лицензии и ограничения. При условии оплаты применимого лицензионного сбора и выполнении условий, изложенных в соответствующем Заказе, NetAlly предоставляет Компании ограниченную, неисключительную, непередаваемую, отзывную лицензию на использование Программного обеспечения и Документации для собственных внутренних деловых целей Компании.

(a) Пробная лицензия: NetAlly настоящим предоставляет Компании временную, неисключительную, непередаваемую, отзывную лицензию на использование пробного продукта, указанного в применяемой NetAlly форме запроса, исключительно для внутреннего тестирования, оценки или демонстрационных целей. Если Компания решит не приобретать лицензию на Пробный продукт, он должен быть удален из системы (систем) Компании, а все разрешенные копии такого Пробного продукта должны быть немедленно уничтожены. Для любого пробного аппаратного продукта необходимо до возврата получить номер разрешения на возврат материалов («RMA #»).

(b) Предварительно выпущенные продукты. Если Продукт, который Компания получила вместе с этой лицензией, еще не является коммерчески доступным («Предварительно выпущенный продукт»), то NetAlly предоставляет Компании временную, неисключительную, не подлежащую передаче, отзывную лицензию на использование Предварительно выпущенного продукта и связанной с ним Документации, если таковая имеется, исключительно для целей внутренней оценки. NetAlly по своему усмотрению может прекратить право Компании использовать Предварительно выпущенный продукт в любое время. Использование Компанией Предварительно выпущенного продукта ограничено тридцатью (30) днями, если иное не согласовано с компанией NetAlly в письменной форме. Компания признает и соглашается с тем, что (i) NetAlly не обещает и не гарантирует Компании, что Предварительно выпущенный продукт будет анонсирован или предоставлен кому-либо в будущем; (ii) NetAlly не имеет явных или подразумеваемых обязательств перед Компанией по анонсированию или представлению Предварительно выпущенного продукта; (iii) NetAlly может не представлять продукт, аналогичный или совместимый с Предварительно выпущенным продуктом; и (iv) любое использование Предварительно выпущенного продукта или любого продукта, связанного с Предварительно выпущенным продуктом, является исключительно собственным риском Компании. В течение срока действия настоящих Общих условий и положений, в случае запроса NetAlly, Компания предоставит NetAlly отзыв об использовании Предварительно выпущенного продукта. Компания не будет раскрывать какие-либо особенности или функции любого Предварительно выпущенного продукта до тех пор, пока NetAlly не сделает Предварительно выпущенный продукт общедоступным.

(c) Лицензия API. NetAlly предоставляет Компании ограниченную, неисключительную, непередаваемую отзывную лицензию на использование API вместе с соответствующей документацией, любыми примерами кода и любыми примерами приложений, предоставляемыми с API, исключительно в связи с Продуктами для внутренних деловых целей Компании; при условии, что Компания не может использовать API в связи с разработкой продукта или услуги, которые конкурируют с Продуктами.

(d) Лицензионные ограничения. За исключением случаев, предусмотренных законом, Компания не будет сама и не станет побуждать или разрешать другим извлекать исходный код Программного обеспечения или осуществлять инженерный анализ, разбирать или декомпилировать Продукты. Компания не имеет права (i) создавать производные работы из Программного обеспечения, (ii) одалживать, сдавать в аренду или лизинг, переуступать, сублицензировать и/или предоставлять через таймшеринговое или сервисное бюро Программное обеспечение, или (iii) передавать Программное обеспечение или предоставлять третьему лицу доступ к Программному обеспечению.

(e) Технологии сторонних производителей. Продукты могут содержать встроенные технологии сторонних производителей («Материалы сторонних производителей»). Такие Материалы лицензированы для использования исключительно с данным Продуктом. Материалы сторонних производителей

предоставляются в соответствии с применимыми условиями использования третьих сторон («Условия использования»). Компания соглашается соблюдать Условия использования и/или получать любые дополнительные лицензии, которые могут потребоваться для использования Материалов сторонних производителей.

(f) Право собственности. Компания NetAlly и ее сторонние лицензиары сохраняют за собой все права, права собственности и интересы в отношении Продуктов, Технологий сторонних производителей и/или API. Компания сохраняет за собой все права, права собственности и интересы в отношении Данных своей компании.

4. Допустимое использование. Компания прямо соглашается ограничить использование Продуктов и/или Услуг теми, которые специально предоставлены в настоящих Общих условиях и положениях. Не ограничивая вышесказанное, Компания прямо соглашается (i) не пытаться проводить инженерный анализ, разбирать, декомпилировать или пытаться получить исходный код Программного обеспечения или любую его часть; (ii) не изменять, переносить, переводить, локализовать или создавать производные работы Программного обеспечения; (iii) не удалять любые уведомления об авторских правах и правах собственности NetAlly или ее поставщиков; (iv) не использовать Продукты для (a) нарушения прав интеллектуальной собственности любой третьей стороны или любых прав на гласность или конфиденциальность; (b) нарушения любого закона, положения, постановления или правила (включая, помимо прочего, законы и постановления, регулирующие экспорт/импорт, недобросовестную конкуренцию, антидискриминацию и/или ложную рекламу); или (c) распространения любого вируса, червей, троянских коней или других программ, предназначенных для повреждения какой-либо системы или данных; и/или (v) не подавать заявки на авторские права или патенты, которые включают Продукт или любую его часть.

5. Данные Компании и личные данные. В течение Срока действия Компания может предоставлять NetAlly свои данные. NetAlly может использовать Данные компании в связи с выполнением своих обязательств в соответствии с настоящими Общими условиями и положениями. Компания настоящим соглашается строго соблюдать все применимые законы о защите данных в отношении передачи, хранения и обработки Персональных данных. Компания признает и соглашается с тем, что в случае передачи Компанией таких Персональных данных компании NetAlly или другим третьим лицам, Компания будет выступать в качестве «Контроллера» таких Персональных данных, как указано в применимых законах о защите данных. Кроме того, в случае нарушения Персональных данных, связанного с действиями или бездействием Компании в при соблюдении настоящих Общих условий и положений, в нарушение Закона о защите данных Компания должна незамедлительно (i) предпринять все необходимые шаги для пресечения такого нарушения; (ii) предпринять все необходимые действия для уменьшения ущерба; (iii) предоставить необходимое уведомление и меры по исправлению положения, как указано в применимом Законе о защите данных; и (iv) содействовать усилиям NetAlly сделать то же самое, исключительно за счет Компании.

6. Срок действия и прекращение действия. Настоящие Общие условия и положения остаются в силе, если они не расторгнуты в соответствии с настоящим Разделом; при условии, что применимый срок подписки для любых лицензий, приобретенных по настоящему Соглашению, будет продолжаться в течение периода времени, указанного в применяемом Предложении. Любая из сторон может прекратить действие настоящих Общих условий и положений немедленно после предоставления письменного уведомления о нарушении другой стороне, если другая сторона существенно нарушает какое-либо из своих обязательств по настоящему Соглашению, но не устраняет такое нарушение в течение 30 (тридцати) дней после получения подобного письменного уведомления. После прекращения действия настоящих Общих условий и положений (i) действие всех лицензий, предоставленных по настоящему Соглашению, немедленно прекращается, (ii) Компания либо вернет Программное обеспечение, Документацию и Копии, либо, с предварительного согласия NetAlly, уничтожит Программное обеспечение, Документацию и Копии.

7. Конфиденциальность. «Конфиденциальная информация» означает любую и всю непубличную техническую, финансовую, коммерческую или другую конфиденциальную или служебную информацию, Услуги, Дорожные карты продуктов, цены, программный код, Документацию, технологии и системы, а также все результаты сравнительного тестирования, запущенного на Продуктах. Ни одна из сторон не будет раскрывать Конфиденциальную информацию какой-либо третьей стороне, за исключением случаев, когда такое раскрытие необходимо для выполнения настоящих Общих условий и положений, или может быть задокументировано, что подобная Конфиденциальная информация находится в общественном достоянии и общедоступна для широкой публики без каких-либо ограничений. Каждая сторона будет защищать Конфиденциальную информацию в той же степени, в какой Компания защищает собственную конфиденциальную информацию, но ни в коем случае не в меньшей степени.

8. Гарантии. NetAlly гарантирует, исключительно в интересах Компании, (i) что Оборудование не будет иметь существенных дефектов в течение двенадцати (12) месяцев после даты отгрузки Оборудования («Гарантийный период на Оборудование»); и (ii) Программное обеспечение будет соответствовать Документации в течение девяноста (90) дней после даты, когда оно впервые стало доступно для загрузки Компанией («Гарантийный срок на программное обеспечение»). Гарантийные обязательства, изложенные в настоящем документе, не распространяются на любой отказ Программного или Аппаратного обеспечения, вызванный (a) несоблюдением Компанией инструкций, процедур или Документации NetAlly по установке, эксплуатации или техническому обслуживанию; (b) ненадлежащим обращением, использованием, небрежностью или неправильной установкой, демонтажем, хранением, обслуживанием или эксплуатацией Продукта Компанией; (c) модификацией или ремонтом без разрешения NetAlly; (d) использованием Продуктов в сочетании с оборудованием или программным обеспечением, не поставляемым NetAlly или не разрешенным в Документации; и/или (e) перебоями в подаче электроэнергии или скачками напряжения, пожаром, наводнением, аварией, действиями третьих лиц или другими событиями, находящимися вне разумного контроля NetAlly. NetAlly не может гарантировать и не гарантирует производительность или результаты, которые могут быть получены при использовании Продуктов, а также не гарантирует, что Продукты подходят для целей Компании или не содержат ошибок. Если в течение Гарантийного срока на программное обеспечение или Гарантийного срока на оборудование о несоответствии будет сообщено в компанию NetAlly, NetAlly по своему усмотрению приложит коммерчески разумные усилия для ремонта или замены несовместимого Программного обеспечения или Оборудования. НАСТОЯЩЕЕ СРЕДСТВО ПРАВОВОЙ ЗАЩИТЫ ЯВЛЯЕТСЯ ЕДИНСТВЕННЫМ И ИСКЛЮЧИТЕЛЬНЫМ СРЕДСТВОМ ЗАКАЗЧИКА, И ЕДИНСТВЕННОЙ ОТВЕТСТВЕННОСТЬЮ NETALLY ЗА НАРУШЕНИЕ ГАРАНТИИ. ЗА ИСКЛЮЧЕНИЕМ ЯВНЫХ ГАРАНТИЙ, УКАЗАННЫХ В ДАННОМ РАЗДЕЛЕ 8. «ГАРАНТИИ» NETALLY ОТКАЗЫВАЕТСЯ ОТ ВСЕХ ГАРАНТИЙ НА ТОВАРЫ, ПРЕДОСТАВЛЯЕМЫЕ ПО НАСТОЯЩЕМУ СОГЛАШЕНИЮ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ ВСЕ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ТОВАРНОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ.

9. ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ. NETALLY НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБЫЕ УБЫТКИ ИЛИ УЩЕРБ, ЕСЛИ ТАКИЕ УБЫТКИ ИЛИ УЩЕРБ НЕ ЯВЛЯЮТСЯ РЕЗУЛЬТАТОМ НЕБРЕЖНОСТИ И/ИЛИ НАМЕРЕННОГО НЕПРАВИЛЬНОГО ПОВЕДЕНИЯ NETALLY. ЕСЛИ NETALLY ПРИЗНАЕТ ОТВЕТСТВЕННОСТЬ, СУММА МАКСИМАЛЬНОЙ ОТВЕТСТВЕННОСТИ NETALLY ЗА ЛЮБЫЕ И ВСЕ УБЫТКИ И/ИЛИ УЩЕРБ (ПО КОНТРАКТУ, ГРАЖДАНСКО-ПРАВОВОМУ ДЕЛИКТУ ИЛИ ИНЫМ УСЛОВИЯМ) НЕ ДОЛЖНЫ ПРЕВЫШАТЬ ОБЩУЮ СУММУ ВСЕХ ЛИЦЕНЗИОННЫХ ПЛАТЕЖЕЙ, ФАКТИЧЕСКИ ОПЛАЧЕННЫХ NETALLY ЗА ВСЕ ПРОДУКТЫ ИЛИ УСЛУГИ В ТЕЧЕНИЕ ШЕСТИ (6) МЕСЯЦЕВ, ПРЕДШЕСТВУЮЩИХ ВОЗНИКНОВЕНИЮ ТАКОЙ ПРЕТЕНЗИИ.

10. ИСКЛЮЧЕНИЕ КОСВЕННЫХ УБЫТКОВ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ ЛЮБАЯ СТОРОНА НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ПЕРЕД ДРУГОЙ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ КОСВЕННЫЕ, НЕПРЯМЫЕ, ОСОБЫЕ, ШТРАФНЫЕ И/ИЛИ СЛУЧАЙНЫЕ УБЫТКИ, ВКЛЮЧАЯ, НО НЕ ТОЛЬКО, ПОТЕРЯНУЮ ПРИБЫЛЬ ИЛИ ПОТЕРЮ ДАННЫХ, ДАЖЕ ЕСЛИ ТАКАЯ СТОРОНА БЫЛА ПРЕДУПРЕЖДЕНА О ВОЗМОЖНОСТИ ПОТЕНЦИАЛЬНЫХ УБЫТКОВ ИЛИ УЩЕРБА.

11. ОСНОВНАЯ ЦЕЛЬ. ЗАЯВЛЕННЫЕ ЗДЕСЬ ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ И ИСКЛЮЧЕНИЕ ОПРЕДЕЛЕННЫХ УБЫТКОВ ПРИМЕНЯЮТСЯ НЕЗАВИСИМО ОТ ДОСТИЖЕНИЯ ОСНОВНОЙ ЦЕЛИ ЛЮБОГО ДЕЙСТВИЯ. ОБЕ СТОРОНЫ ЗДЕСЬ ЧЕТКО ПОДТВЕРЖДАЮТ, ЧТО ЭТИ ОГРАНИЧЕНИЯ ОТВЕТСТВЕННОСТИ ОТРАЖЕНЫ В ЦЕНАХ.

12. Компенсация. По любым претензиям, основанным на нарушении Компанией Раздела 3 «Предоставление лицензии и ограничения», Раздела 4 «Допустимое использование», Раздела 5 «Компания и личные данные», Раздела 7 «Конфиденциальность», Раздела 8 «Гарантии», Раздела 14.4 «Соблюдение требований и экспортный контроль», Раздела 14.6 «Борьба с коррупцией и взяточничеством» и/или использование Продукта (ов) Компанией, Компания настоящим соглашается возместить, защитить и обезопасить NetAlly от таких претензий за счет Компании и возместить все убытки, которые окончательно назначит суд компетентной юрисдикции, при условии, что NetAlly (i) незамедлительно уведомит Компанию о претензиях в письменной форме; (ii) позволяет Компании контролировать защиту или любые связанные с этим переговоры по урегулированию; и (iii) сотрудничает с Компанией в защите любых таких претензий; при условии, что Компания не повлияет на урегулирование, если такое урегулирование не предоставит NetAlly полное освобождение от ответственности.

13. Отношения с третьими сторонами. Отношения между сторонами, установленные настоящими Общими условиями и положениями, являются отношениями независимых подрядчиков, и ничто, содержащееся в настоящих Общих условиях и положениях, не должно толковаться как: (i) предоставление одной из сторон

полномочий направлять или контролировать повседневную деятельность другой стороны; (ii) возможность представлять стороны как партнеров, совместные предприятия, совладельцев или иным образом как участников совместного или общего предприятия или франшизы; (iii) возможность для Компании создавать или принимать какие-либо обязательства от имени NetAlly для любых целей; или (iv) разрешение любому покупателю, конечному пользователю или другому физическому или юридическому лицу, не являющемуся стороной настоящих Общих условий и положений, считаться сторонним бенефициаром настоящих Общих условий и положений.

14. Общие положения.

14.1 Полнота соглашения Условий и положений и интеграция. Эти Общие условия и положения и все приложения, ссылающиеся на эти Общие положения и условия, представляют собой полное соглашение между сторонами по предмету настоящего Соглашения и заменяют собой все предыдущие обсуждения, соглашения и договоренности любого рода и характера между сторонами. Ни одна из сторон не может считаться разработчиком настоящих Общих условий и положений. Никакие изменения настоящих Общих условий и положений не будут иметь силы, если они не внесены в письменной форме и не подписаны обеими сторонами. Все дополнительные и противоречащие положения и условия, представленные вместе или в любом сообщении, включая, помимо прочего, Заказ на поставку Компании, за исключением цены, количества и местоположения, которые указаны в Заказе на поставку, настоящим отклоняются и считаются недействительными.

14.2 Независимость положений и сохраняемость. Незаконность или неисполнимость любого положения настоящих Общих условий и положений не влияет на действительность и исковую силу каких-либо юридических и подлежащих исполнению положений настоящего Соглашения. Если какое-либо положение настоящих Общих условий и положений будет сочтено неисполнимым судом компетентной юрисдикции, то такое положение должно быть переработано для обеспечения максимальной защиты, предоставляемой законом, в соответствии с целью применимого положения. Любое положение, содержащееся в настоящем документе, которое по своей природе должно оставаться в силе после прекращения действия настоящих Общих условий и положений, должно оставаться в силе, включая, помимо прочего, Раздел 7 «Конфиденциальность», Раздел 9 «Ограничение ответственности и исключение косвенных убытков», Раздел 12 «Возмещение ущерба», и Раздел 14 «Общие положения».

14.3 Переуступка прав. Ни одна из сторон не может уступать какие-либо права или делегировать какие-либо обязательства по настоящему Соглашению, будь то в силу закона или иным образом, за исключением случая продажи бизнеса любой из сторон путем слияния, продажи активов, продажи акций или иным образом, или за исключением случаев письменного согласия другой стороны, в котором не будет необоснованно отказано. Эти Общие условия и положения связывают стороны, их соответствующие участвующие дочерние компании, аффилированные лица, правопреемников и разрешенных правопреемников.

14.4 Соблюдение нормативных требований и экспортный контроль. Компания обязуется полностью соблюдать все применимые законы, правила и постановления, в том числе законы США, а также любых других юрисдикций по всему миру, которые применяются к коммерческой деятельности Компании в связи с настоящими Общими условиями и положениями. Компания признает, что Продукты NetAlly и/или Услуги NetAlly регулируются законами правительства США о контроле за экспортом. Компания обязуется соблюдать все применимые законы экспортного контроля, получать все применимые экспортные лицензии и не будет экспортировать или реэкспортировать какую-либо часть Продуктов и/или Услуг в любую страну в нарушение таких ограничений или в любую страну, которая может подпадать под действие эмбарго со стороны правительства Соединенных Штатов, или конечным пользователям, принадлежащим или связанным со странами, на которые наложено эмбарго со стороны правительства Соединенных Штатов.

14.5. Уведомление об использовании для правительства США. Программное обеспечение NetAlly является «Коммерческим объектом» в соответствии с определением этого термина в 48 C.F.R. § 2.101, состоящим из «Коммерческого компьютерного программного обеспечения» и «Документации по коммерческому компьютерному программному обеспечению», как эти термины используются в 48 C.F.R. § 12.212 и 48 C.F.R. § 227.7202, если применимо. В соответствии с 48 C.F.R. § 12.212 и 48 C.F.R. § 227.7202-1 – 227.7202-4, Коммерческое компьютерное программное обеспечение и Документация по коммерческому компьютерному программному обеспечению лицензируются для конечных пользователей в правительстве США (a) только как Коммерческие элементы и (b) только с теми правами, которые предоставлены всем другим конечным пользователям в соответствии с положениями и условиями, изложенными в настоящем документе. Для некоторых компонентов Программного обеспечения,

указанных в Приложениях, это Программное обеспечение и Документация предоставляются на ОГРАНИЧЕННОЙ основе. Использование, копирование или раскрытие информации правительством США подлежит ограничениям, изложенным в подпунктах (c) (1) и (2) Ограниченных прав на коммерческое компьютерное программное обеспечение в 48 CFR 52.227-19, в зависимости от обстоятельств.

14.6 Борьба с коррупцией и взяточничеством. Компания не будет производить или разрешать совершать какие-либо ненадлежащие платежи и будет соблюдать Закон США о борьбе с коррупцией за рубежом, Закон Великобритании о взяточничестве, Конвенцию Организации экономического сотрудничества и развития («ОЭСР») о борьбе с взяточничеством и другие применимые местные законы о борьбе с взяточничеством и международные стандарты борьбы со взяточничеством. Компания заявляет и гарантирует, что она не будет выплачивать комиссию, вознаграждение за поисковые или справочные услуги, а также вносить какие-либо политические взносы любому лицу в связи с деятельностью от имени NetAlly.

14.7 Применимое право и решение споров. Стороны прямо соглашаются, что Конвенция ООН о международной купле-продаже товаров, Единый закон о транзакциях с компьютерной информацией («UCITA») и Международные коммерческие условия, изданные Международной торговой палатой («Инкотермс»), не применяются ни к каким и всем действиям, совершенным любой из сторон по настоящему Соглашению в соответствии с настоящими Общими положениями и условиями. Настоящие Общие условия и положения и все вытекающие из них претензии и/или встречные иски регулируются, истолковываются и исполняются в соответствии с законами штата Колорадо, Соединенные Штаты Америки, без рассмотрения дела третейским судьей и/или с использованием принципов коллизионного права. Стороны прямо соглашаются с тем, что исключительной юрисдикцией в отношении любых и всех возникающих претензий и/или встречных исков, вытекающих из настоящих Общих условий и положений, являются федеральные и местные суды Денвера, штат Колорадо.

14.8 Форс-мажор. Ни одна из сторон не несет ответственности за невыполнение или задержку в предоставлении Услуг или любых других обязательств в соответствии с настоящими Общими условиями и положениями, а также за любой ущерб, понесенный другой стороной или Конечным пользователем в результате такого отказа или задержки, которая прямо или косвенно связана с событием, выходящим за рамки предсказуемого контроля такой стороны, включая, помимо прочего, забастовки, беспорядки, стихийные бедствия, террористические акты, вмешательство правительства или другие стихийные бедствия, или любые другие причины, находящиеся вне разумного контроля такой стороны.

14.9 Отказ. Каждая сторона соглашается с тем, что отказ другой стороны в любое время потребовать выполнения такой стороной любого из положений настоящего документа не означает отказ этой стороны от прав требовать неукоснительного выполнения тех же или аналогичных положений или любых других положений настоящего Соглашения позднее.

15. Уведомления. Все уведомления в соответствии с настоящими Общими условиями и положениями должны составляться на английском языке в письменной форме и отправляться по адресу, указанному на титульной странице, либо (i) заказной авиапочтой; (ii) срочной доставкой (на следующий день) через уважаемого стороннего курьера; или (iii) по электронной почте с получением «уведомления о прочтении» и «уведомления о доставке». В отношении получения NetAlly электронного уведомления, указанного в пункте (iii) выше, такое уведомление будет считаться полученным только после того, как Компания получит подтверждение «уведомления о прочтении» и «уведомления о доставке», и такое уведомление будет действительным только в том случае, если оно отправлено на адрес legal@netally.com.

Смотрите также https://www.netally.com/web-legal/.

Лицензия на функцию поддержки декодирования верхнего уровня

Стандартная общественная лицензия GNU
Версия 2, Июнь 1991

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Всем позволяется копировать и распространять дословные копии этого лицензионного документа, но его изменение запрещено.

[Это первая выпущенная версия библиотеки GPL. Она имеет номер 2, потому что соответствует версии 2 обычной GPL.]

Преамбула

Лицензии для большинства программных продуктов разработаны таким образом, чтобы лишить вас свободы изменять и делиться им с другими. Стандартная общественная лицензия GNU, напротив, направлена на то, чтобы гарантировать вам свободу делиться и изменять свободные программы; это способно обеспечить уверенность, что программы свободны для всех их пользователей.
Эта Стандартная общественная лицензия применима к большинству программ, распространяемых Фондом свободного программного обеспечения (Free Software Foundation), и к любому другому программному обеспечению, чьи авторы захотят ее использовать. Вы тоже можете применить ее к своим программам.

Говоря о свободном программном обеспечении (free software), мы имеем в виду свободу, а не цену. Наша Стандартная общественная лицензия была разработана, чтобы обеспечить уверенность в том, что у вас есть свобода распространять копии свободного программного обеспечения (и брать плату за эту услугу, если хотите), что вы получили исходный код программы или можете его получить, если пожелаете, что вы вправе внести изменения в программу или использовать ее части в новых свободных программах; и что вам известно о наличии прав на это.

Для защиты ваших прав нам необходимо предусмотреть ограничения, которые бы запретили любому отказать вам в ваших правах или потребовать вас отказаться от них. Эти ограничения выражаются в определенных накладываемых на вас обязанностях в случае, если вы распространяете копии программного обеспечения или вносите в него изменения.

Например, если вы распространяете копии такой программы, вне зависимости от того, бесплатно или за деньги, вы обязаны предоставить получателям все права, которыми обладаете сами. Вы обязаны убедиться, что и они тоже получили или могут получить исходный код. Если вы связываете программу с библиотекой, то должны предоставить получателям полные объектные файлы, чтобы они могли повторно связать их с библиотекой после внесения изменений в библиотеку и ее перекомпиляции. Также вы обязаны довести до их сведения эти положения, чтобы они знали о своих правах.

Мы защищаем ваши права в два этапа: (1) защищаем авторские права на программное обеспечение, и (2) предоставляем эту лицензию, дающую законное разрешение копировать, распространять и/или вносить изменения в программное обеспечение.

Кроме того, для защиты каждого дистрибьютора нам необходимо удостовериться в том, что все понимают отсутствие гарантии на свободное программное обеспечение. Если программа была изменена кем-то другим и передана далее, необходимо, чтобы его получатели знали, что то, что они получили, не является оригиналом. Таким образом, любые проблемы, вызванные третьими лицами, не отразятся на репутации автора оригинальной программы.

И, наконец, любая свободная программа постоянно подвергается угрозе со стороны патентов на программное обеспечение. Нам хотелось бы избежать опасности того, что кто-то из распространителей свободной программы в индивидуальном порядке получит патентные права с целью сделать программу своей собственностью. Для предотвращения этого мы ясно дали понять, что любой патент должен предусматривать свободное его использование всеми, либо не регистрироваться вовсе.

На большую часть программного обеспечения GNU, включая некоторые библиотеки, распространяется стандартная общественная лицензия GNU, которая была разработана для служебных программ. Эта лицензия, GNU Library General Public License, применяется к определенным указанным библиотекам. Эта

лицензия в значительной мере отличается от обычной лицензии; обязательно прочитайте ее полностью и не предполагайте, что ее содержание такое же, как у обычной лицензии.

Причина, по которой у нас есть отдельная общедоступная лицензия для некоторых библиотек, заключается в том, что она стирает различие, которое мы обычно проводим между изменением или дополнением программы и простым ее использованием. Связывание программы с библиотекой без изменения библиотеки в некотором смысле означает простое использование библиотеки и аналогично запуску служебной программы или прикладной программы. Однако в текстовом и юридическом смысле связанный исполняемый файл является комбинированным произведением, производным от исходной библиотеки, и обычная Стандартная общественная лицензия рассматривает его как таковой.

Из-за этого нечеткого различия применение обычной Стандартной общественной лицензии для библиотек не способствовало эффективному продвижению совместного использования программного обеспечения, поскольку большинство разработчиков не использовали библиотеки. Мы пришли к выводу, что менее жесткие условия могут способствовать лучшему совместному использованию.

Однако неограниченное связывание несвободных программ лишило бы пользователей этих программ всех преимуществ свободного статуса самих библиотек. Эта Стандартная общественная лицензия для библиотек предназначена для того, чтобы разрешить разработчикам платных программ использовать свободные библиотеки, сохраняя при этом вашу свободу как пользователя таких программ изменять свободные библиотеки, которые в них включены. (Мы не видели, как этого добиться в отношении изменений в файлах заголовков, но мы достигли этого в отношении изменений фактических функций библиотеки.) Надеемся, что это приведет к более быстрому развитию свободных библиотек.

Ниже приводятся точные условия копирования, распространения и внесения изменений. Обратите особое внимание на разницу между «произведением, основанным на библиотеке» и «произведением, использующим библиотеку». Первое содержит код, полученный из библиотеки, а второе работает только вместе с библиотекой.
Обратите внимание, что на библиотеку может распространяться обычная Стандартная общественная лицензия, а не эта специальная.

УСЛОВИЯ КОПИРОВАНИЯ, РАСПРОСТРАНЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ

0. Это лицензионное соглашение распространяется на любую программу или иную работу, содержащую помещенное владельцем авторских прав уведомление, указывающее на распространение этой работы в соответствии с условиями Стандартной общественной лицензии (также называется «настоящая Лицензия»). Под «вы» понимается обращение к каждому лицензиату.
Термин «библиотека» означает набор программных функций и/или данных, подготовленных для удобной связи с прикладными программами (которые используют некоторые из этих функций и данных) для формирования исполняемых файлов.
Приведенный ниже термин «Библиотека» относится к любой такой программной библиотеке или произведению, которые были распространены в соответствии с этими условиями. «Произведение, основанное на Библиотеке» означает саму Библиотеку или любую производную работу в соответствии с законом об авторском праве, то есть произведение, содержащее Библиотеку или ее часть, дословно или с изменениями и/или прямо переведенную на другой язык. (Здесь и далее перевод включается без ограничений в термин «изменения».)
«Исходный код» произведения означает предпочтительную форму произведения для внесения в него изменений. Для библиотеки полный исходный код означает весь исходный код для всех содержащих его модулей, плюс все связанные файлы определения интерфейса, а также скрипты, используемые для компиляции управления и установки библиотеки.

Деятельность, отличная от копирования, распространения и внесения изменений, данной Лицензией не охватывается; эта деятельность находится вне зоны ее действия. Акт запуска программы с использованием Библиотеки не запрещен, а результаты работы программы подпадают под действие лицензии, только если их содержимое составляет произведение, основанное на Библиотеке (вне зависимости, было ли оно выполнено с использованием Библиотеки). Так ли это, зависит от того, что делает Библиотека, и что делает программа, которая ее использует.

1. Вы вправе копировать и распространять неизмененные копии исходного кода Библиотеки в том виде, в каком их получили, на любом носителе и по любым каналам, при условии, что вы открыто и соответствующим образом приведете в каждой копии заявление об авторских правах и отказ от гарантийных обязательств; оставите без изменений все заявления, относящиеся к данной лицензии и к

отсутствию гарантий; и предоставите всем получателям вместе с самой Библиотекой и копию данной Лицензии.
Вы вправе брать плату за акт физической передачи копии, вы вправе также, по своему желанию, предоставлять гарантийные обязательства в обмен на плату.

2. Вы вправе вносить изменения в свою копию или копии Библиотеки, а также любую ее часть, тем самым создавая произведение, основанное на Библиотеке; а также копировать и распространять эти изменения или произведение в соответствии с условиями приведенного выше Раздела 1, при условии, что выполнены все приведенные ниже требования:
a) Измененное произведение должно само по себе быть библиотекой программ.
b) Вы обязаны обеспечить наличие уведомления в измененных файлах, указывающее на факт изменения этих файлов, с датой внесения изменения.
c) Вы обязаны обеспечить полностью бесплатное лицензирование для всех третьих сторон, в соответствии с условиями данной лицензии, любой распространяемой или публикуемой вами работы.
d) Если средство в измененной Библиотеке относится к функции или таблице данных, которые должны быть предоставлены прикладной программой, которая использует это средство, кроме как аргумент, передаваемый при вызове средства, тогда вы должны предпринять добросовестные усилия, чтобы гарантировать, что в случае, если приложение не предоставляет такую функцию или таблицу, средство по-прежнему будет работать и выполнять ту часть своего назначения, которая остается значимой.
(Например, функция в библиотеке для вычисления квадратного корня имеет цель, которая полностью определена независимо от приложения. Поэтому в подразделе 2d требуется, чтобы любая предоставляемая приложением функция или таблица, используемая этой функцией, была необязательной: если приложение не предоставляет его, функция извлечения квадратного корня все равно должна вычислять квадратные корни.)

Эти требования относятся ко всему модифицированному произведению целиком. Если идентифицируемые участки этого произведения не являются производными от Библиотеки, и могут сами рассматриваться как независимые и отдельные произведения, тогда эта Лицензия и ее положения к ним не применимы, при условии, что вы распространяете их как отдельные произведения. Но когда вы распространяете эти же части произведения как части целого, являющегося произведением, основанным на Библиотеке, такое распространение должно соответствовать положениям данной Лицензии, по которой права других лицензиатов распространяются на все целое, независимо от того, кто его написал.

Таким образом, цель данного раздела состоит не в том, чтобы заявить свои права или оспорить ваши права на произведение, написанное целиком вами; скорее, целью является обеспечить право управлять распространением производных или коллективных произведений, основанных на Библиотеке.
Кроме того, простое совмещение другого произведения, не основанного на Библиотеке, с самой Библиотекой (или произведением, основанном на Библиотеке) на носителе информации или в среде передачи данных не переносит другое произведение под действие данной Лицензии.

3. Вы можете применить условия обычной Стандартной общественной лицензии GNU вместо данной Лицензии к конкретной копии Библиотеки. Для этого вы должны изменить все примечания, относящиеся к этой Лицензии, так, чтобы они относились к обычной Стандартной общественной лицензии GNU версии 2 вместо настоящей Лицензии. (Если появилась более новая версия, чем версия 2 обычной Стандартной общественной лицензии GNU, вы можете указать эту версию, если хотите.) Не вносите никаких других изменений в эти уведомления.
После внесения этого изменения в данную копию оно становится необратимым для этой копии, поэтому обычная Стандартная общественная лицензия GNU применяется ко всем последующим копиям и производным работам, сделанным из этой копии.
Эта опция полезна, если вы хотите скопировать часть кода Библиотеки в программу, которая не является библиотекой.

4. Вы можете копировать и распространять Библиотеку (или ее часть или производную в соответствии с Разделом 2) в объектном коде или исполняемой форме в соответствии с условиями Разделов 1 и 2 выше при условии, что вы прилагаете к ней полный соответствующий машиночитаемый исходный код, который должен распространяться в соответствии с условиями приведенных выше Разделов 1 и 2 на носителе, обычно используемом для обмена программным обеспечением.
Если распространение объектного кода осуществляется путем предоставления доступа для копирования из указанного места, то предоставление эквивалентного доступа для копирования исходного кода из того же места удовлетворяет требованию по распространению исходного кода, даже если третьи стороны не обязаны копировать исходный код вместе с объектным кодом.

5. Программа, которая не содержит производных от какой-либо части Библиотеки, но предназначена для работы с Библиотекой путем компиляции или связывания с ней, называется «произведением, использующим Библиотеку». Такое произведение, само по себе, не является производной от Библиотеки и поэтому не входит в сферу действия настоящей Лицензии.
Однако при связывании «произведения, использующего Библиотеку» с Библиотекой создается исполняемый файл, который является производным от Библиотеки (поскольку он содержит части Библиотеки), а не «произведение, использующее Библиотеку». Таким образом, исполняемый файл подпадает под действие настоящей Лицензии. Условия распространения таких исполняемых файлов изложены в Разделе 6.
Когда «произведение, использующее Библиотеку» использует материал из файла заголовка, который является частью Библиотеки, объектный код для произведения может быть производным от Библиотеки произведением, даже если исходный код таковым не является. Это особенно важно, если произведение можно связать без Библиотеки или если произведение само является библиотекой. Порог для истинности этого не определен законом точно.
Если в таком объектном файле используются только числовые параметры, макеты структур данных и средства доступа, а также небольшие макросы и небольшие встроенные функции (длиной десять или менее строк), то использование объектного файла не имеет ограничений, независимо от того, является ли он юридически производной работой. (Исполняемые файлы, содержащие этот объектный код плюс части Библиотеки, по-прежнему подпадают под действие Раздела 6.)
В противном случае, если произведение является производным от Библиотеки, вы можете распространять объектный код произведения в соответствии с положениями Раздела 6. Любые исполняемые файлы, содержащие это произведение, также подпадают под Раздел 6, независимо от того, связаны они непосредственно с самой Библиотекой или нет.

6. В качестве исключения из приведенных выше Разделов вы также можете скомпилировать или связать «произведение, использующее Библиотеку» с Библиотекой для создания произведения, содержащего части Библиотеки, и распространять это произведение на условиях по вашему выбору, при условии, что Условия допускают внесение изменений в произведение для собственного использования и инженерный анализ для отладки таких изменений.
С каждой копией произведения вы должны предоставлять заметное уведомление о том, что в ней используется Библиотека, и что Библиотека и ее использование подпадают под действие настоящей Лицензии. Вы должны предоставить копию этой Лицензии. Если во время выполнения произведения отображаются уведомления об авторских правах, вы должны включить в них уведомление об авторских правах на Библиотеку, а также ссылку, указывающую пользователю на копию этой Лицензии. Кроме того, вы должны сделать одно из следующего:
a) Сопроводить произведение полным соответствующим машиночитаемым исходным кодом Библиотеки, включая любые изменения, использованные в произведении (которые должны распространяться в соответствии с приведенными выше Разделами 1 и 2); и, если произведение представляет собой исполняемый файл, связанный с Библиотекой, с полным машиночитаемым «произведением, использующим Библиотеку» в качестве объектного кода и/или исходного кода, чтобы пользователь мог изменить Библиотеку, а затем повторно связать ее для создания измененного исполняемого файла, содержащего измененную Библиотеку. (Понятно, что пользователь, который изменяет содержимое файлов определений в Библиотеке, не обязательно сможет перекомпилировать приложение для использования измененных определений.)
b) Сопроводить произведение письменным предложением, действительным в течение как минимум трех лет, предоставить тому же пользователю материалы, указанные в Подразделе 6a выше, за плату, не превышающую стоимости выполнения этого распространения.
c) Если распространение произведения осуществляется путем предоставления доступа к копии из указанного места, предложите эквивалентный доступ для копирования указанных выше материалов из того же места.
d) Убедитесь, что пользователь уже получил копию этих материалов или что вы уже отправили этому пользователю копию.

Для исполняемого файла необходимая форма «произведения, использующего Библиотеку» должна включать в себя любые данные и служебные программы, необходимые для воспроизведения исполняемого файла из него. Однако в качестве особого исключения распространяемый исходный код не обязательно должен включать в себя что-либо, что обычно распространяется (в исходной или двоичной форме) с основными компонентами (компилятор, ядро и т.д.) операционной системы, в которой выполняется исполняемый файл, если только этот компонент не сопровождает исполняемый файл.
Может случиться так, что это требование противоречит лицензионным ограничениям других проприетарных библиотек, которые обычно не входят в комплект поставки. Такое противоречие означает, что вы не можете использовать их и Библиотеку вместе в исполняемом файле, который распространяете.

7. Вы можете размещать библиотечные объекты, которые являются произведением на основе Библиотеки, бок о бок в одной библиотеке вместе с другими библиотечными средствами, не подпадающими под действие настоящей Лицензии, и распространять такую объединенную библиотеку, при условии, что раздельное распространение произведения на основе Библиотеки и других библиотечных средств разрешено иным образом, и при условии, что вы выполняете следующее:
a) Сопровождаете объединенную библиотеку копией того же произведения, основанного на Библиотеке, без каких-либо других библиотечных средств. Это должно быть распространено в соответствии с условиями приведенных выше Разделов.
b) Делаете заметное примечание к объединенной библиотеке о том, что часть ее является произведением, основанным на Библиотеке, и объясняете, где найти сопутствующую несоединенную форму того же произведения.

8. Вы не можете копировать, изменять, сублицензировать, связывать или распространять Библиотеку, за исключением случаев, прямо предусмотренных настоящей Лицензией. Любая попытка каким-либо иным образом копировать, изменять, сублицензировать, связывать или распространять Библиотеку запрещается и автоматически прекращает ваши права по данной Лицензии. Однако у сторон, получивших от вас копии или права по данной Лицензии, не будет прекращено действие лицензий до тех пор, пока такие стороны полностью соблюдают правила.

9. Вы не обязаны принимать эту Лицензию, поскольку вы ее не подписывали. Однако ничто иное не дает вам разрешения на изменение или распространение Библиотеки или производных от нее произведений. Если вы не принимаете данную Лицензию, эти действия запрещены законом. Таким образом, изменяя или распространяя Библиотеку (или любое произведение, основанное на Библиотеке), вы подтверждаете свое согласие с данной Лицензией и всеми ее условиями для копирования, распространения или изменения Библиотеки или произведений на ее основе.

10. Каждый раз, когда вы распространяете Библиотеку (или любое произведение, основанное на Библиотеке), получатель автоматически получает от первоначального лицензиара лицензию на копирование, распространение, связывание или изменение Библиотеки в соответствии с настоящими условиями. Вы не имеете права накладывать какие-либо дополнительные ограничения на осуществление получателями прав, предоставленных здесь. Вы не несете ответственности за обеспечение соблюдения этой Лицензии третьими сторонами.

11. Если в результате судебного решения или заявления о нарушении патентных прав или по любой другой причине (не ограничиваясь патентными вопросами), вам навязываются условия (по решению суда, соглашению или иным образом), которые противоречат условиям настоящей Лицензии, они не освобождают вас от выполнения условий данной Лицензии. Если вы не можете распространять Библиотеку таким образом, чтобы одновременно выполнять свои обязательства по данной Лицензии и любые другие соответствующие обязательства, то, как следствие, вы вообще не можете распространять Библиотеку. Например, если патентная лицензия не разрешает бесплатное распространение Библиотеки всеми теми, кто получает копии прямо или косвенно через вас, то единственный способ удовлетворить и ее, и данную Лицензию - это полностью воздержаться от распространения Библиотеки.
Если какая-либо часть этого раздела будет признана недействительной или не имеющей исковой силы при каких-либо конкретных обстоятельствах, предполагается, что остальная часть раздела будет применяться, а раздел в целом будет предназначен для применения в других обстоятельствах.
Целью этого раздела не является побуждение вас к нарушению каких-либо требований к патентам или другим правам собственности или к оспариванию правомочности любых таких требований; этот раздел имеет единственную цель - защитить целостность системы распространения свободного программного обеспечения, которая реализуется с помощью практики общедоступных лицензий. Многие люди внесли щедрый вклад в широкий спектр программного обеспечения, распространяемого через эту систему, полагаясь на ее последовательное применение. Только автор должен решить, готов ли он или она распространять программное обеспечение через любую другую систему, и лицензиат не может навязывать такой выбор.
Этот раздел предназначен для того, чтобы полностью прояснить, что считается последствием остальной части данной Лицензии.

12. Если распространение и/или использование Библиотеки ограничено в определенных странах патентами или защищенными авторскими правами интерфейсами, первоначальный владелец авторских прав, который размещает Библиотеку под этой Лицензией, может добавить явное ограничение географического распространения, исключающее эти страны, чтобы распространение было разрешено

только в странах, не исключенных таким образом, или между ними. В таком случае данная Лицензия включает ограничение, как если бы оно было написано в ее тексте.

13. Free Software Foundation может время от времени публиковать исправленные и/или новые версии Стандартной общественной лицензии для Библиотеки. Такие новые версии будут по духу аналогичны текущей версии, но могут отличаться в деталях, призванных решить определенные новые проблемы.
Каждая версия имеет собственный номер. Если в Библиотеке имеется номер версии применяемой к ней Лицензии и указано «любая более поздняя версия», у вас есть возможность следовать условиям либо этой версии, либо любой более поздней версии, опубликованной Free Software Foundation. Если в Библиотеке не указан номер версии лицензии, вы можете выбрать любую версию, когда-либо опубликованную Free Software Foundation.

14. Если вы хотите включить части Библиотеки в другие свободно распространяемые программы, условия распространения которых несовместимы с условиями распространения Библиотеки, напишите автору и попросите разрешения. Для программного обеспечения, авторское право на которое принадлежит Free Software Foundation, пишите в Free Software Foundation; иногда мы делаем для этого исключения. Наше решение будет руководствоваться двумя целями: сохранением свободного статуса всех производных нашего свободного программного обеспечения и поощрением совместного использования и повторного использования программного обеспечения в целом.

ГАРАНТИЯ ОТСУТСТВУЕТ

15. ПОСКОЛЬКУ БИБЛИОТЕКА ПРЕДОСТАВЛЯЕТСЯ С БЕСПЛАТНОЙ ЛИЦЕНЗИЕЙ, НА НЕЕ НЕ ПРЕДОСТАВЛЯЕТСЯ КАКАЯ-ЛИБО ГАРАНТИЯ В СТЕПЕНИ, РАЗРЕШЕННОЙ ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ. КРОМЕ ТЕХ СЛУЧАЕВ, КОГДА ИНОЕ ЗАЯВЛЕНО В ЯВНОЙ ПИСЬМЕННОЙ ФОРМЕ, ДЕРЖАТЕЛИ АВТОРСКИХ ПРАВ И/ИЛИ ДРУГИЕ СТОРОНЫ ПРЕДОСТАВЛЯЮТ БИБЛИОТЕКУ «КАК ЕСТЬ» БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ТОВАРНОЙ ГОДНОСТИ И ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННЫХ ЦЕЛЕЙ. ВЕСЬ РИСК, КАСАЮЩИЙСЯ КАЧЕСТВА И РАБОТЫ БИБЛИОТЕКИ ЛЕЖИТ НА ВАС. В ТОМ СЛУЧАЕ, КОГДА БИБЛИОТЕКА ОКАЗЫВАЕТСЯ ДЕФЕКТНОЙ, ВЫ НЕСЕТЕ РАСХОДЫ НА ВСЕ НЕОБХОДИМОЕ ОБСЛУЖИВАНИЕ, РЕМОНТ ИЛИ ИСПРАВЛЕНИЕ.

16. В ЛЮБОМ СЛУЧАЕ, КРОМЕ ТЕХ, КОГДА ТРЕБУЕТСЯ СО СТОРОНЫ ПРИМЕНИМОГО ЗАКОНОДАТЕЛЬСТВА ИЛИ СОГЛАСОВАНО В ПИСМЕННОЙ ФОРМЕ, ЛЮБОЙ ВЛАДЕЛЕЦ АВТОРСКИХ ПРАВ ИЛИ ЛЮБАЯ ДРУГАЯ СТОРОНА, КОТОРАЯ МОЖЕТ ВНОСИТЬ ИЗМЕНЕНИЯ И/ИЛИ ИЗМЕНЯТЬ РАСПРОСТРАНЕНИЕ БИБЛИОТЕКИ, КАК РАЗРЕШЕНО ВЫШЕ, НЕ НЕСЕТ ПЕРЕД ВАМИ НИКАКОЙ ОТВЕТСТВЕННОСТИ ЗА ЛЮБОЙ УЩЕРБ, ВКЛЮЧАЯ ОТВЕТСТВЕННОСТЬ ЗА СЛУЧАЙНЫЕ ИЛИ КОСВЕННЫЕ УБЫТКИ, ВЫЗВАННЫЕ ИСПОЛЬЗОВАНИЕМ ИЛИ НЕВОЗМОЖНОСТЬЮ ИСПОЛЬЗОВАТЬ БИБЛИОТЕКУ (ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ, ПОТЕРЮ ДАННЫХ ИЛИ ДАННЫЕ, ПРЕДОСТАВЛЕННЫЕ НЕТОЧНО, ИЛИ УБЫТКИ, ПОЛУЧЕННЫЕ ВАМИ ИЛИ ТРЕТЬИМИ СТОРОНАМИ, ИЛИ НЕВОЗМОЖНОСТЬ РАБОТЫ БИБЛИОТЕКИ С ЛЮБЫИ ДРУГИМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ), ДАЖЕ ЕСЛИ ТАКОМУ ДЕРЖАТЕЛЮ ПРАВ ИЛИ ДРУГОЙ СТОРОНЕ СООБЩАЛОСЬ О ВОЗМОЖНОСТИ ТАКИХ УБЫТКОВ.

КОНЕЦ УСЛОВИЙ

Как применить эти условия к вашим новым библиотекам

Если вы разрабатываете новую библиотеку и хотите, чтобы она была максимально полезной для общественности, мы рекомендуем сделать ее свободным программным обеспечением, которое каждый может распространять и изменять. Вы можете сделать это, разрешив распространение в соответствии с этими условиями (или, в качестве альтернативы, в соответствии с условиями обычной Стандартной общественной лицензии).
Для применения этих условий прикрепите к библиотеке следующие уведомления. Безопаснее всего прикрепить их к началу каждого исходного файла, чтобы наиболее эффективно передать отказ от гарантии; и в каждом файле должна быть хотя бы строка «авторское право» и указатель на то, где находится полное уведомление.

Эта библиотека является свободным программным обеспечением; вы можете распространять и/или изменять его в соответствии с условиями Стандартной общественной лицензии для библиотеки GNU, опубликованной Free Software Foundation; либо версии 2 Лицензии, либо (по вашему выбору) любой более поздней версии.

Эта библиотека распространяется в надежде, что она будет полезна, но БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ; даже без подразумеваемых гарантий ТОВАРНОЙ ГОДНОСТИ или ПРИГОДНОСТИ ДЛЯ КОНКРЕТНОЙ ЦЕЛИ. Подробнее смотрите Стандартную общественную лицензию для библиотеки GNU.

Вы должны были получить копию Стандартной общественной лицензии GNU вместе с этой библиотекой; Если нет, напишите в Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA. Также добавьте информацию о том, как с вами связаться по электронной и бумажной почте.

Вы также должны попросить своего работодателя (если вы работаете программистом) или вашу школу, если таковая имеется, подписать «отказ от авторских прав» для библиотеки, если это необходимо.

Авторское право Iperf2

Mark Gates (Марк Гейтс), Ajay Tirumala (Аджай Тирумала), Jim Ferguson (Джим Фергюсон), Jon Dugan (Джон Дуган), Feng Qin (Фэн Цинь), Kevin Gibbs (Кевин Гиббс), John Estabrook (Джон Эстэбрук), National Laboratory for Applied Network Research (Национальная лаборатория прикладных сетевых исследований), National Center for Supercomputing Applications (Национальный центр суперкомпьютерных приложений), University of Illinois at Urbana-Champaign (Иллинойский университет в Урбана-Шампейн), http://www.ncsa.uiuc.edu

Авторское право David Young

ВОЗНИКШИХ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ В СЛУЧАЕ ОСВЕДОМЛЕННОСТИ О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.

Авторское право A. Onoe и S. Leffler

Авторское право (c) 2001 год, Atsushi Onoe
Авторское право (c) 2002 – 2005 годы, Sam Leffler, Errno Consulting
Все права защищены.

Распространение и использование в исходной или двоичной форме, с внесением изменений или без них, разрешено при соблюдении следующих условий*:

1. При распространении исходного кода должно сохраняться указанное выше уведомление об авторском праве*, этот список условий и приведенный ниже отказ от ответственности.
2. При распространении в виде двоичного кода в документации и/или других материалах, поставляемых с дистрибутивом, должно быть воспроизведено указанное выше уведомление об авторском праве, этот список условий и приведенный ниже отказ от ответственности.
3. Имя автора не может использоваться для поддержки или продвижения продуктов, созданных на базе этого программного обеспечения, без предварительного письменного разрешения.

Кроме того, это программное обеспечение может распространяться в соответствии с условиями лицензии GNU General Public License («GPL») версии 2, опубликованной Free Software Foundation.

ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЯЕТСЯ АВТОРОМ «КАК ЕСТЬ», И БЕЗ ЛЮБЫХ ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЮЩИХСЯ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ, ГАРАНТИИ КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КОНКРЕТНОЙ ЦЕЛИ. НИ В КОЕМ СЛУЧАЕ АВТОР НЕ БУДЕТ НЕСТИ КАКУЮ-ЛИБО ОТВЕТСТВЕННОСТЬ ЗА ЛЮБОЙ ПРЯМОЙ, КОСВЕННЫЙ, СПЕЦИАЛЬНЫЙ, ШТРАФНОЙ ИЛИ ЛЮБОЙ ДРУГОЙ УЩЕРБ (ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ, ПРИОБРЕТЕНИЕ ТОВАРОВ ИЛИ УСЛУГ ДЛЯ ЗАМЕНЫ, ПОТЕРЮ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ, ПОТЕРЮ ДАННЫХ ИЛИ ПРИБЫЛИ, А ТАКЖЕ ПРЕРЫВАНИЕ КОММЕРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ) ПО ЛЮБОЙ ПРИЧИНЕ И ТЕОРИИ ОТВЕТСТВЕННОСТИ, БУДЬ ТО ПО УСЛОВИЯМ КОНТРАКТА, ПРЯМОЙ ОТВЕТСТВЕННОСТИ ИЛИ ГРАЖДАНСКОМУ ПРАВОНАРУШЕНИЮ (ВКЛЮЧАЯ ХАЛАТНОСТЬ И Т.П.), ВОЗНИКШИХ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ В СЛУЧАЕ ОСВЕДОМЛЕННОСТИ О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.

Авторское право S.Leffler

Авторское право (c) 2002 – 2005 годы, Sam Leffler, Errno Consulting
Все права защищены.

Распространение и использование в исходной или двоичной форме, с внесением изменений или без них, разрешено при соблюдении следующих условий:

1. При распространении исходного кода должно сохраняться указанное выше уведомление об авторском праве, этот список условий и приведенный ниже отказ от ответственности.
2. При распространении в виде двоичного кода в документации и/или других материалах, поставляемых с дистрибутивом, должно быть воспроизведено указанное выше уведомление об авторском праве, этот список условий и приведенный ниже отказ от ответственности.
3. Имя автора не может использоваться для поддержки или продвижения продуктов, созданных на базе этого программного обеспечения, без предварительного письменного разрешения.

Кроме того, это программное обеспечение может распространяться в соответствии с условиями лицензии GNU General Public License («GPL») версии 2, опубликованной Free Software Foundation.

ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЯЕТСЯ АВТОРОМ «КАК ЕСТЬ», И БЕЗ ЛЮБЫХ ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЮЩИХСЯ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ, ГАРАНТИИ КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КОНКРЕТНОЙ ЦЕЛИ. НИ В КОЕМ СЛУЧАЕ АВТОР НЕ БУДЕТ НЕСТИ КАКУЮ-ЛИБО ОТВЕТСТВЕННОСТЬ ЗА ЛЮБОЙ ПРЯМОЙ, КОСВЕННЫЙ, СПЕЦИАЛЬНЫЙ, ШТРАФНОЙ ИЛИ ЛЮБОЙ ДРУГОЙ УЩЕРБ (ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ, ПРИОБРЕТЕНИЕ ТОВАРОВ ИЛИ УСЛУГ ДЛЯ ЗАМЕНЫ, ПОТЕРЮ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ, ПОТЕРЮ ДАННЫХ ИЛИ ПРИБЫЛИ, А ТАКЖЕ ПРЕРЫВАНИЕ КОММЕРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ) ПО

ЛЮБОЙ ПРИЧИНЕ И ТЕОРИИ ОТВЕТСТВЕННОСТИ, БУДЬ ТО ПО УСЛОВИЯМ КОНТРАКТА, ПРЯМОЙ ОТВЕТСТВЕННОСТИ ИЛИ ГРАЖДАНСКОМУ ПРАВОНАРУШЕНИЮ (ВКЛЮЧАЯ ХАЛАТНОСТЬ И Т.П.), ВОЗНИКШИХ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ В СЛУЧАЕ ОСВЕДОМЛЕННОСТИ О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.

Авторское право B. Paul

Распространение и использование в исходной или двоичной форме, с внесением изменений или без них, разрешено при соблюдении следующих условий:

1. При распространении исходного кода должно сохраняться указанное выше уведомление об авторском праве, этот список условий и приведенный ниже отказ от ответственности.
2. При распространении в виде двоичного кода в документации и/или других материалах, поставляемых с дистрибутивом, должно быть воспроизведено указанное выше уведомление об авторском праве, этот список условий и приведенный ниже отказ от ответственности.
3. Все рекламные материалы, в которых упоминаются функции или использование данного программного обеспечения, должны содержать следующее уведомление:

   Данный продукт включает программное обеспечение, разработанное Bill Paul.
4. Ни имя автора, ни имена любых его партнеров, не могут использоваться для поддержки или продвижения продуктов, созданных на базе этого программного обеспечения, без предварительного письменного разрешения.

ЭТО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЯЕТСЯ BILL PAUL И ДРУГИМИ УЧАСТНИКАМИ «КАК ЕСТЬ», И БЕЗ ЛЮБЫХ ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЮЩИХСЯ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ, ГАРАНТИИ КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КОНКРЕТНОЙ ЦЕЛИ. НИ В КОЕМ СЛУЧАЕ BILL PAUL НЕ БУДЕТ НЕСТИ КАКУЮ-ЛИБО ОТВЕТСТВЕННОСТЬ ЗА ЛЮБОЙ ПРЯМОЙ, КОСВЕННЫЙ, СПЕЦИАЛЬНЫЙ, ШТРАФНОЙ ИЛИ ЛЮБОЙ ДРУГОЙ УЩЕРБ (ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ, ПРИОБРЕТЕНИЕ ТОВАРОВ ИЛИ УСЛУГ ДЛЯ ЗАМЕНЫ, ПОТЕРЮ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ, ПОТЕРЮ ДАННЫХ ИЛИ ПРИБЫЛИ, А ТАКЖЕ ПРЕРЫВАНИЕ КОММЕРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ) ПО ЛЮБОЙ ПРИЧИНЕ И ТЕОРИИ ОТВЕТСТВЕННОСТИ, БУДЬ ТО ПО УСЛОВИЯМ КОНТРАКТА, ПРЯМОЙ ОТВЕТСТВЕННОСТИ ИЛИ ГРАЖДАНСКОМУ ПРАВОНАРУШЕНИЮ (ВКЛЮЧАЯ ХАЛАТНОСТЬ И Т.П.), ВОЗНИКШИХ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ДАЖЕ В СЛУЧАЕ ОСВЕДОМЛЕННОСТИ О ВОЗМОЖНОСТИ ТАКОГО УЩЕРБА.

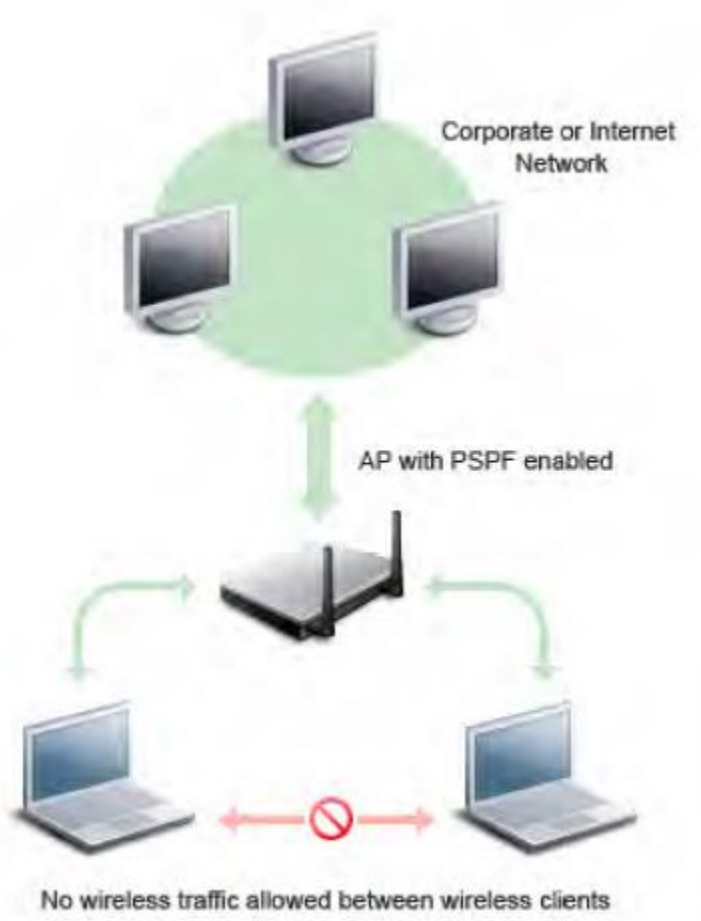
Политика

AP With Encryption Disabled (Точка доступа с отключенным шифрованием)

Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer предупреждает администратора о любой точке доступа, работающей без каких-либо механизмов шифрования данных WLAN уровня 2, таких как WEP, TKIP или AES. Технологии VPN на уровне 3 и выше являются наиболее часто используемой альтернативой механизмам шифрования данных уровня 2 WLAN. Если ни один из механизмов шифрования не используется, данные, которыми обмениваются точка доступа и ее клиентские станции, могут быть перехвачены злоумышленниками. Типично для точки доступа, работающей без какого-либо механизма шифрования, что могут быть неавторизованные клиенты без ключей шифрования, которые способны связываться с точкой доступа и получать доступ к проводной сети предприятия. Это не только ставит под угрозу конфиденциальность данных пользователя, но и подвергает риску доступ к корпоративной проводной сети.

Этот сигнал тревоги может быть отключен для гостевой беспроводной сети предприятия или для развертываний публичных точек доступа, где шифрование обычно не требуется. Однако можно рассмотреть возможность включения сигнала тревоги PSPF (Publicly Secure Packet Forwarding – Безопасность публичной передачи пакетов) для защиты своей незашифрованной беспроводной сети. PSPF - это функция, реализованная в точках доступа WLAN для блокировки связи беспроводных клиентов с другими беспроводными клиентами.



Corporate or Internet Network	Корпоративная сеть или сеть Интернет
AP with PSPF enabled	Точка доступа с включенной функцией PSPF
No wireless traffic allowed between wireless clients	Между беспроводными клиентами недопустим никакой беспроводный трафик

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает устройства, не использующие шифрование, и рекомендует пользователю использовать более надежные механизмы шифрования. Для большинства сред WLAN беспроводные клиенты взаимодействуют только с такими устройствами, как веб-серверы в проводной сети. Включение функции PSPF (Publicly Secure Packet Forwarding – Безопасность публичной передачи пакетов) позволяет защитить беспроводных клиентов от взлома беспроводными устройствами злоумышленника. Функция PSPF эффективна для защиты беспроводных клиентов в беспроводных сетях общего пользования (публичных точках доступа), например, в аэропортах, отелях, кафе, университетских кампусах и т.д., где аутентификация не имеет значения и к точкам доступа может подключаться любой. Функция PSPF предотвращает непреднамеренный обмен файлами одних клиентских устройств с другими клиентскими устройствами в беспроводной сети.

Client With Encryption Disabled (Клиент с отключенным шифрованием)

Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer предупреждает администратора о любой клиентской станции, работающей без каких-либо механизмов шифрования данных WLAN уровня 2, таких как WEP, TKIP или AES. Технологии VPN на уровне 3 и выше являются наиболее часто используемой альтернативой механизмам шифрования данных уровня 2 WLAN. Если не используется ни один из механизмов шифрования, данные, которыми обмениваются точка доступа и ее клиентские станции, могут быть перехвачены злоумышленниками. Клиенты с отключенным протоколом WEP рискуют своей файловой системой, которая может содержать конфиденциальную корпоративную информацию и к которой злоумышленники могут получить доступ. Затем эти клиенты могут выступать для злоумышленников точкой входа в корпоративную сеть.

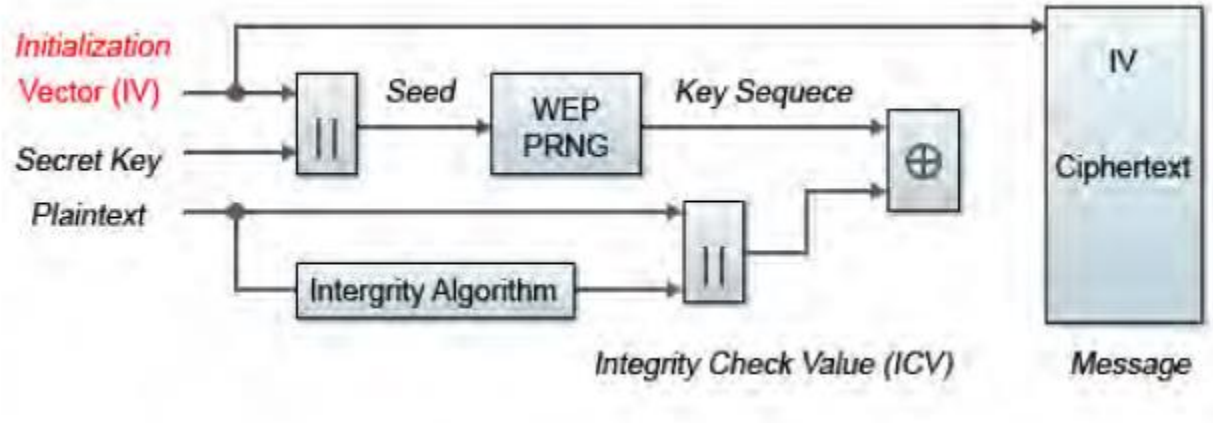
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает устройства, которые не используют шифрование, и рекомендует пользователю использовать более надежные механизмы шифрования.

WEP IV Key Reused (Ключ WEP IV использован повторно)

Описание сигнала тревоги и возможные причины

Хорошо известно, что устройство WLAN, использующее для шифрования статический ключ WEP, уязвимо для различных атак взлома WEP (Обратитесь к документу «Weaknesses in the Key Scheduling Algorithm of RC4 – I» (Слабые стороны алгоритма планирования ключей RC4 – I), авторы Scott Fluhrer, Itsik Mantin и Adi Shamir (Скотт Флурер, Ицик Мантин и Ади Шамир)).



Initialization Vector (IV)	Вектор инициализации (IV)
Seed	Сид
Key Sequence	Последовательность ключа
Secret Key	Секретный ключ
Plaintext	Открытый текст

Integrity Algorithm	Алгоритм целостности
Ciphertext	Зашифрованный текст
Integrity Check Value (ICV)	Значение проверки целостности (ICV)
Message	Сообщение

Блок-схема процесса шифрования WEP

Взлом секретного ключа WEP приводит к отсутствию защиты шифрованием, что ставит под угрозу конфиденциальность данных. Ключ, вводимый в 64-битный или 128-битный алгоритм шифрования WEP, состоит из секретного ключа, сконфигурированного пользователем, соединенного с 24-битным IV (вектором инициализации). IV определяется передающей станцией. Когда ключ IV повторно используется часто или в последовательных кадрах, это увеличивает вероятность восстановления секретного ключа хакерами, проникающими в беспроводную сеть.

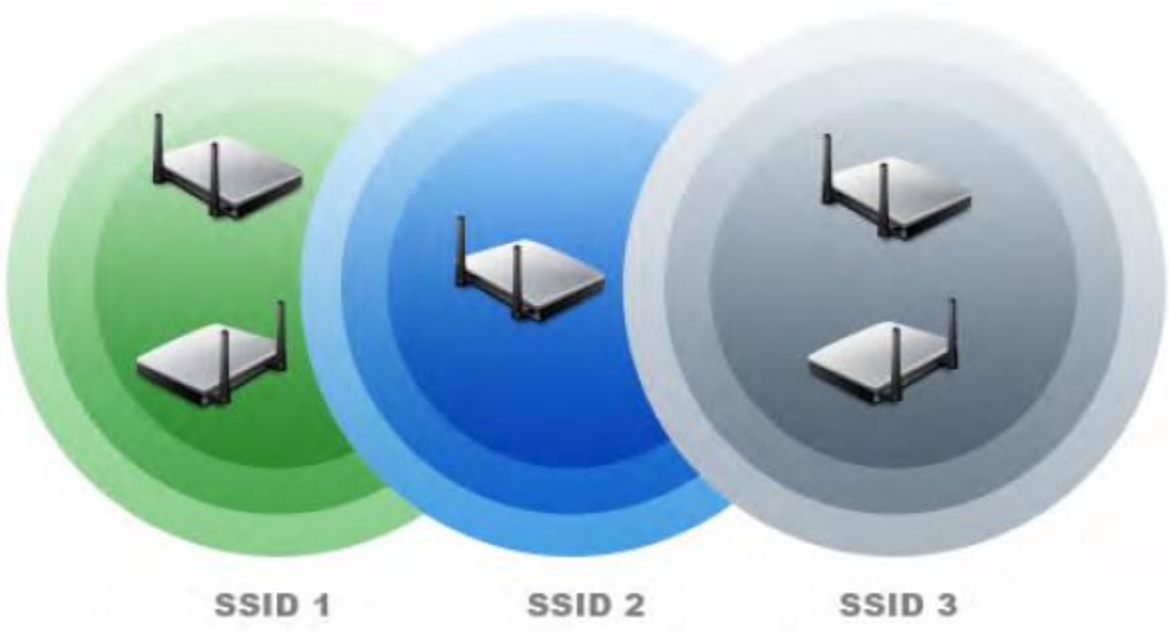
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer предупреждает о слабой реализации WEP и для устранения проблемы с использованием IV рекомендует обновить прошивку устройства, запросив ее у производителя устройства. В идеале корпоративную сеть WLAN можно защитить от уязвимости WEP с помощью шифрования TKIP (Temporal Key Integrity Protocol – Протокол ограниченной по времени целостности ключа), которое поддерживается большинством беспроводного оборудования корпоративного уровня. Устройства с поддержкой TKIP не подвержены атаке по ключу WEP.

Insufficient RF Coverage (Недостаточное радиочастотное покрытие)

Описание сигнала тревоги и возможные причины

Обследование площадки развертывания сети WLAN позволяет обеспечить достаточное радиочастотное покрытие (с заданным пользователем минимальным уровнем радиочастотного сигнала) с использованием, по крайней мере, одной точки доступа для обслуживания предполагаемой зоны покрытия. Из-за динамического характера радиочастотной среды фактическая зона покрытия может время от времени меняться. Например, если будут перемещены стены или перегородки (которые могут вызывать помехи) или если будут введены новые устройства, которые также работают в диапазоне 2,4 ГГц (беспроводные телефоны, микроволновые печи и т.п.), создаваемое точками доступа радиочастотное покрытие может быть нарушено. Если такое изменение станет существенным, беспроводные клиенты не только испытают снижение уровня производительности, но могут столкнуться даже с проблемами подключения.



Приложение AirMagnet Enterprise отслеживает радиочастотное покрытие нескольких сетей WLAN по их идентификатору SSID

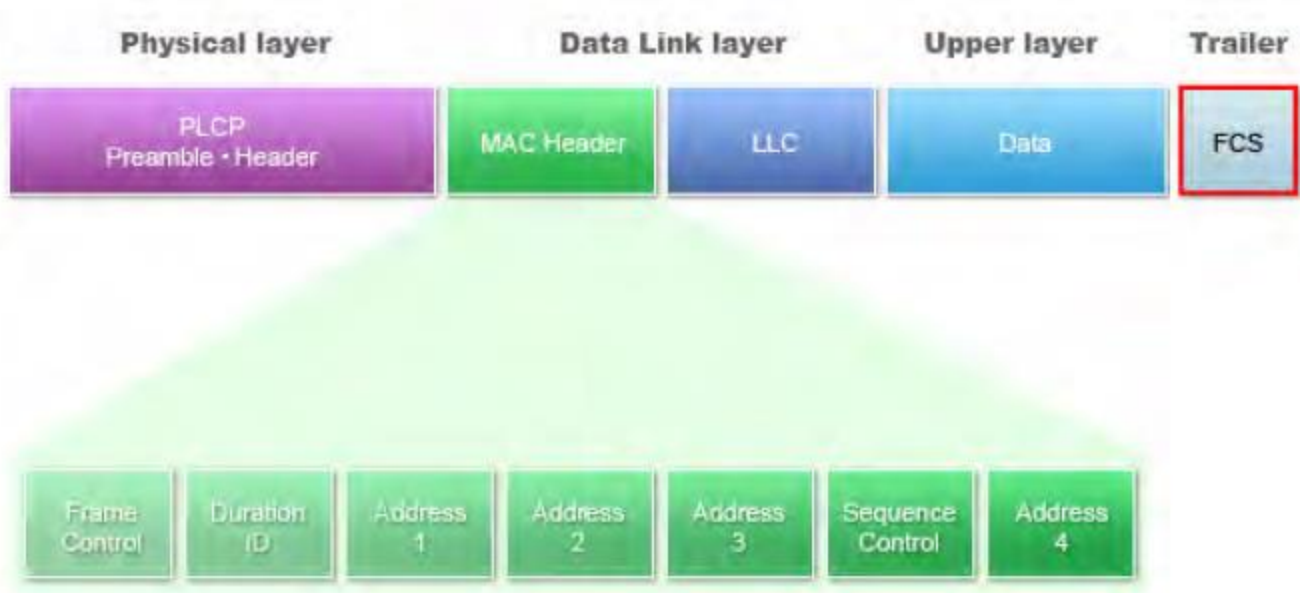
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает несколько сетей WLAN по их идентификаторам SSID, чтобы убедиться, что зона каждой сети SSID в достаточной степени покрывается в данном месте хотя бы одной точкой доступа. Когда приложение AirMagnet WiFi Analyzer обнаруживает какой-либо SSID, не соответствующий заданной пользователем минимальной мощности сигнала точки доступа, то подает сигнал тревоги «Недостаточное радиочастотное покрытие» (Insufficient RF Coverage). Для исправления ситуации можно установить дополнительные точки доступа в зоне SSID или устранить источники помех.

Excessive Packet Errors (Чрезмерное количество ошибок пакетов)

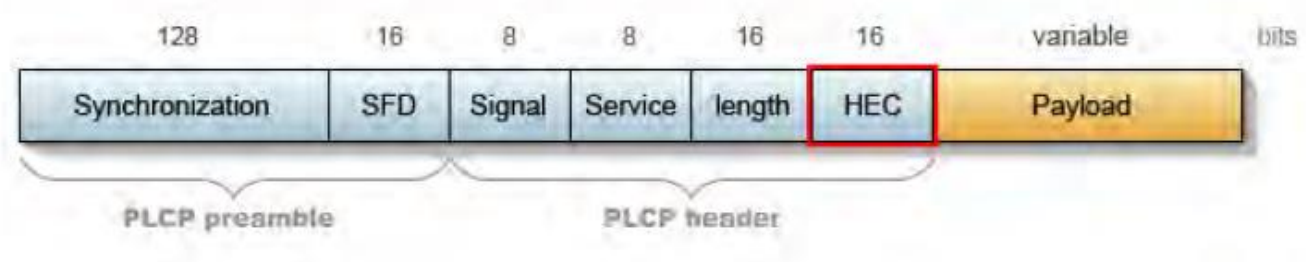
Описание сигнала тревоги и возможные причины

Радиочастотный спектр сети WLAN является открытым, динамическим, совместно используемым, подверженным шумам, помехам, коллизиям пакетов, многолучевому распространению, синдрому скрытых узлов и т.д. IEEE 802.11 имеет встроенный механизм проверки ошибок, позволяющий обнаруживать ошибки передачи и приема, вызванные любой из вышеупомянутых проблем. Например, спецификация физического уровня IEEE 802.11b DSSS (Direct Sequence Spread Spectrum – Расширение спектра по методу прямой последовательности) включает в заголовок PLCP (Physical Layer Convergence Protocol – Протокол сходимости физического уровня) поля HEC (Header Error Check - Проверка ошибок заголовка) для обнаружения ошибок (смотрите рисунок ниже). Приемник выполняет вычисления в полях синхронизации, обслуживания и длины и сравнивает их с переданным значением. Если результаты не совпадают, получатель должен принять решение об аварийном завершении кадра.



Physical Layer	Физический уровень
Data Link Layer	Уровень канала передачи данных
Upper Layer	Верхний уровень
Trailer	Концевик
Preamble – Header	Преамбула – Заголовок
MAC Header	Заголовок MAC
Data	Данные
Frame Control	Управление кадром
Duration ID	Идентификатор продолжительности
Address	Адрес
Sequence Control	Управление последовательностью

Кадр IEEE 802.11 включает контрольную сумму в PLCP и FCS для заголовка кадра и тела кадра соответственно



Synchronization	Синхронизация
Signal	Сигнал
Service	Служба
Length	Длина
Variable bits	Переменное количество битов
Payload	Полезная нагрузка
PLCP preamble	Преамбула PLCP
PLCP header	Заголовок PLCP

HEC (Контрольная сумма ошибки заголовка), заданная в заголовке PLCP

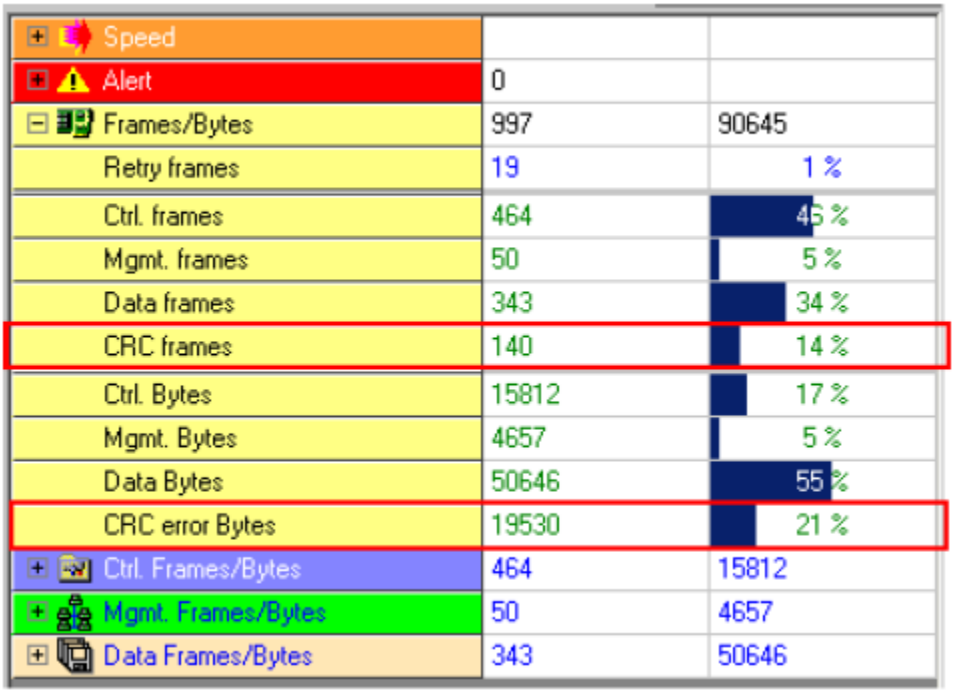
Протокол уровня MAC 802.11 для обнаружения ошибок также задает поле FCS (Frame Checksum - Контрольная сумма кадра) в конце пакета. Смотрите таблицу ниже.

Управление кадром	Идентификатор продолжительности	Адрес 1 (источник)	Адрес 2 (адресат)	Адрес 3 (узел приема)	Последовательное управление	Адрес 4 (узел передачи)	Данные	FCS
2	2	6	6	6	2	6	0 – 2312	4

FCS (Контрольная сумма кадра), задаваемая в формате протокола MAC 802.11

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает эти кадры с ошибками и отслеживает их в зависимости от устройства и ориентации канала. Смотрите рисунок ниже:



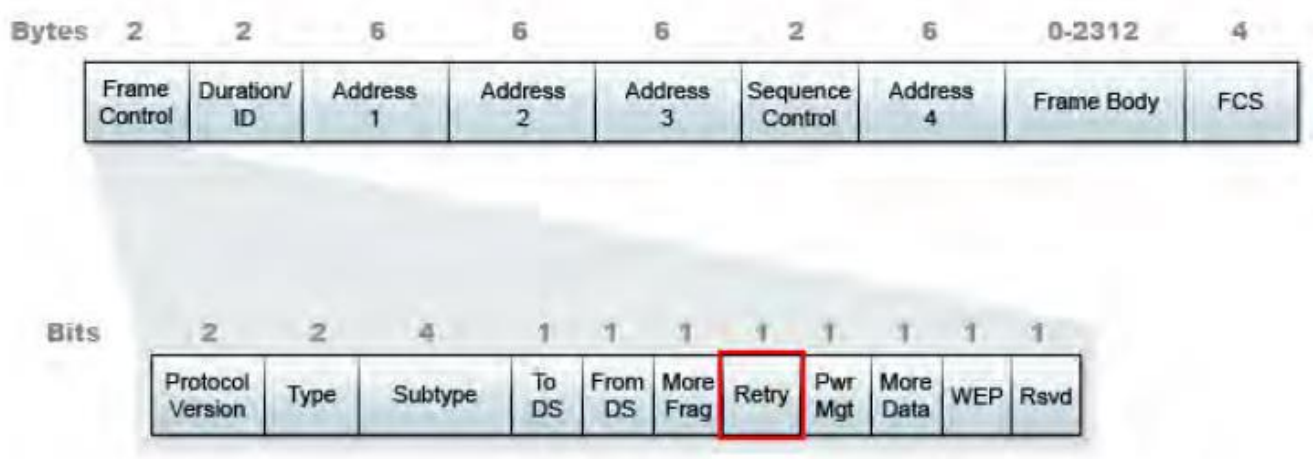
Отображение отслеживания ошибок кадра CRC приложением AirMagnet WiFi Analyzer для канала или устройства

Когда отношение кадров с ошибкой CRC к общему количеству кадров превышает определяемое пользователем пороговое значение, приложение AirMagnet WiFi Analyzer предупреждает администратора о возможных проблемах с производительностью сети WLAN.

Excessive Frame Retries (Чрезмерное количество повторных попыток передачи кадра)

Описание сигнала тревоги и возможные причины

Радиочастотный спектр сети WLAN является открытым, динамическим, совместно используемым, подверженным шумам, помехам, коллизиям пакетов, многолучевому распространению, синдрому скрытых узлов и т.д. При появлении ошибок, вызванных любой из вышеперечисленных проблем, передатчик кадра с ошибкой не получит кадр управления 802.11, называемый кадром подтверждения. При отсутствии подтверждения передатчик предполагает, что приемник не принял кадр успешно, и повторно передает неподтвержденный кадр с битом повтора (Retry) в кадре, установленным на единицу. Это указывает на повторную передачу. На рисунке ниже показано поле Retry в заголовке кадра 802.11.

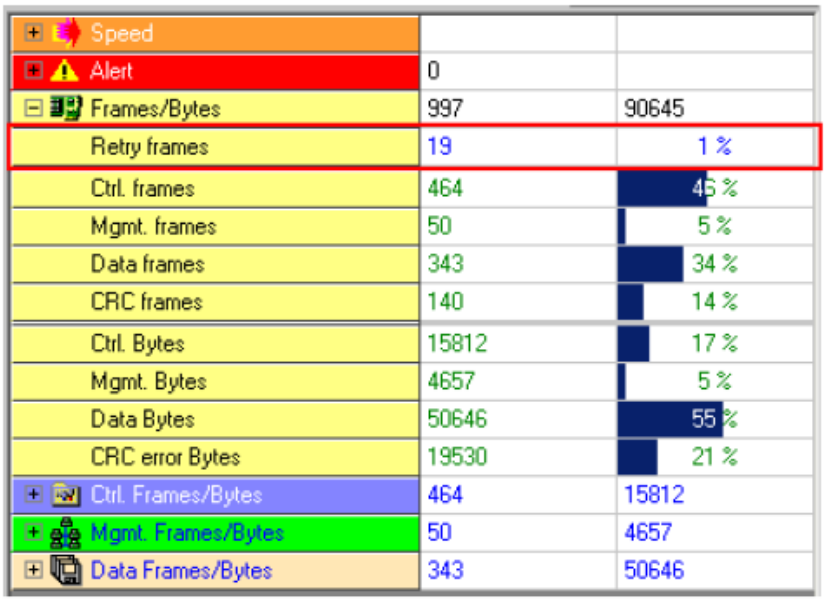


Bytes	Байты
Frame Control	Управление кадром
Duration ID	Идентификатор продолжительности
Address	Адрес
Sequence Control	Управление последовательностью
Frame Body	Тело кадра
Bits	Биты
Protocol Version	Версия протокола
Type	Тип
Subtype	Подтип
To DS	К DS
From DS	От DS
More Fragm	Больше фрагментов
Retry	Повторная попытка
Pwr Mgt	Управление мощностью
More Data	Больше данных
Rsvd	Зарезервировано

Заголовок кадра 802.11, включающий поле Retry для индикации повторной передачи кадра

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает кадры повтора и отслеживает их для каждого устройства и ориентации канала. Смотрите рисунок ниже:



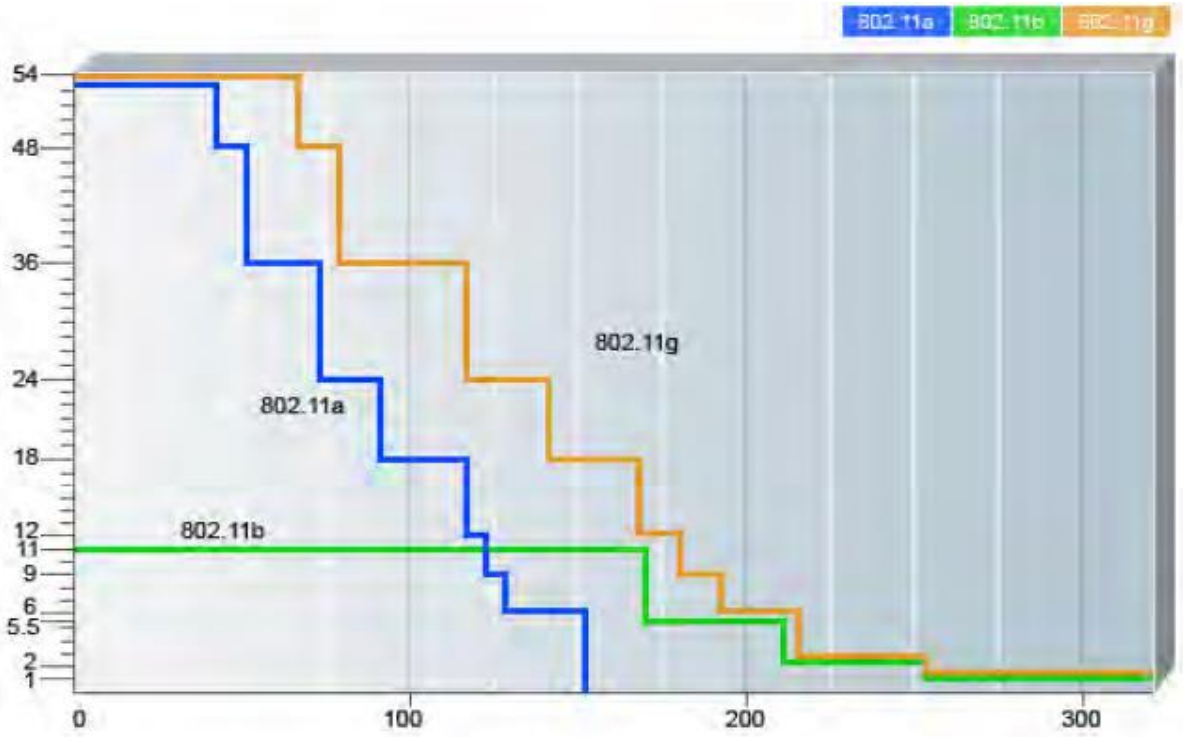
Отображение приложением AirMagnet WiFi Analyzer отслеживания кадров с ошибкой Retry (повторная попытка) для канала или устройства

Когда отношение количество повторных попыток передачи кадров к общему количеству кадров превышает заданное пользователем пороговое значение, приложение AirMagnet WiFi Analyzer предупреждает администратора о возможной проблеме производительности WLAN из-за шумов, помех, коллизий пакетов, многолучевого распространения, синдрома скрытого узла и т.д. После этого администратор получает возможность предпринять соответствующие шаги, чтобы избежать подобных проблем. Например, если проблема возникает из-за шумов или помех, для отслеживания и устранения основной причины можно использовать инструмент поиска Find приложения AirMagnet WiFi Analyzer.

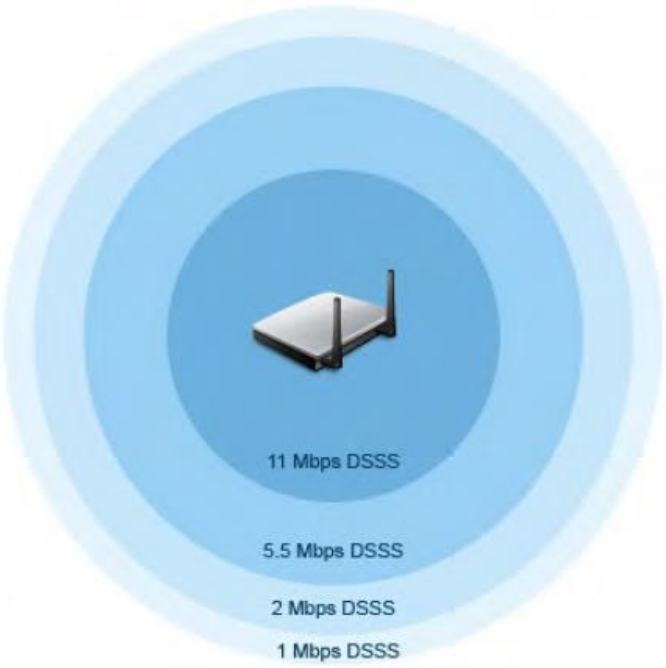
Excessive Low Speed Transmission (Чрезмерно низкая скорость передачи)

Описание сигнала тревоги и возможные причины

Устройства стандартов 802.11a, 11b или 11g от кадра к кадру используют несколько различных скоростей передачи. Более высокая скорость передачи требует меньшей полосы пропускания и обеспечивает более высокую пропускную способность. Оптимизация скорости передачи является ключевым фактором в процессе обследования площадки и развертывания сети WLAN. Обычно это зависит от качества сигнала и расстояния.



Корреляция скорости и расстояния для 802.11 a/b/g



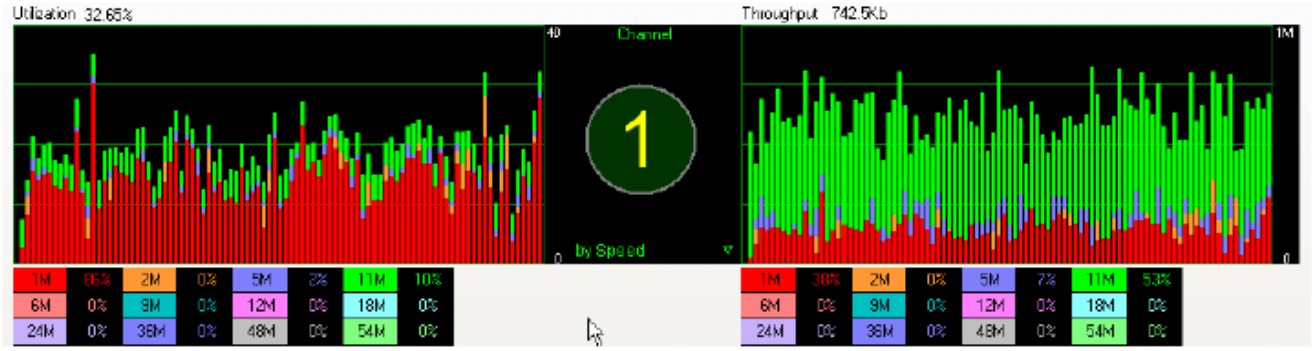
Корреляция скорости и покрытия для 802.11b

В таблице ниже указаны все поддерживаемые скорости и то, что приложение AirMagnet WiFi Analyzer считает низкой скоростью для выбранного стандарта.

Скорость	802.11b (Мбит/с)	802.11g (Мбит/с)	802.11a (Мбит/с)
Поддерживаемая скорость	1, 2, 5.5, 11	1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 54	6, 9, 12, 24, 36, 48, 54
AirMagnet Enterprise считает низкой скоростью	1, 2	1, 2, 5.5, 6, 9, 11, 12, 24, 36	6, 9, 12, 24, 36

Поддерживаемые скорости передачи и те из них, которые приложение Wi-Fi AirMagnet Analyzer считает «низкой» скоростью

Однако для достижения такого же низкого уровня ошибок по сравнению с низкоскоростной передачей высокоскоростная передача требует более высокого качества сигнала. Выбор скорости передачи – это решение, принимаемое передатчиком, который также обнаруживает проблемы приема из-за отсутствия подтверждений. Для повышения надежности передатчик может изменять скорость передачи. Если этот сценарий применяется слишком часто, сеть WLAN замедляется и ее пропускная способность ухудшается. Обратите внимание на проблему, показанную на скриншоте экрана приложения AirMagnet WiFi Analyzer ниже. Там показана чрезмерно низкая скорость передачи (1 Мбит/с), высокая степень использования (32%) и низкая пропускная способность (931 Кбит/с).



Скриншот экрана Channel (Канал) приложения AirMagnet WiFi Analyzer, показывающий взаимосвязь использования полосы пропускания (Bandwidth Utilization), пропускной способности (Throughput) и скорости передачи (Transmit Speed)

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer предупредит администратора, если увидит большой объем трафика на более низких скоростях, что может привести к чрезмерному использованию полосы пропускания и снижению пропускной способности. Администратор должен предпринять соответствующие шаги, чтобы повысить качество сигнала для получения более высоких скоростей передачи. Также важно отметить, что во избежание снижения скорости передачи расстояние от станций до точки доступа должно быть подходящим.

Device Using Open Authentication (Устройство, использующее открытую аутентификацию)

Описание сигнала тревоги и возможные причины

В наши дни для защиты сетей WLAN широко используется открытая аутентификация 802.11 (Open Authentication) (в отличие от аутентификации с совместно используемым ключом (Shared-key)) в сочетании с таким протоколом аутентификации более высокого уровня, как 802.1x. В некоторых сетях, где для вызова клиентских станций, пытающихся установить связь с точкой доступа, вместо открытой аутентификации со статическим ключом WEP используется аутентификация с совместно используемым ключом. С другой стороны, открытая аутентификация принимает соединения от любого клиента, и идентификация клиента не проверяется. Аутентификация с совместно используемым ключом кажется более безопасной, но на

самом деле оказалась уязвимой для взлома ключа WEP злоумышленниками, поскольку текст запроса и ответ являются четкими и не зашифрованными. Это означает, что информация легко перехватывается и интерпретируется любым пользователем с соответствующим программным обеспечением.

Решение AirMagnet

Рекомендуется использовать открытую аутентификацию 802.11 с определенными механизмами аутентификации более высокого уровня, такими как структура 802.1x/EAP или VPN. Если в вашей сети решено использовать аутентификацию с совместно используемым ключом или что-то иное, кроме открытой аутентификации, можно включить этот сигнал тревоги, чтобы приложение AirMagnet Mobile предупреждало вас всякий раз, когда обнаруживает любое устройство, нарушающее вашу политику развертывания и не использующее открытую аутентификацию.

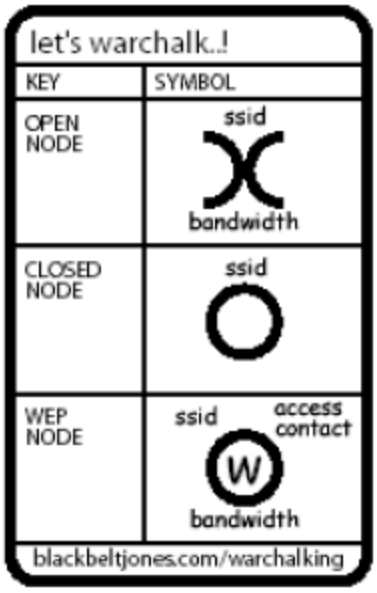
Device Probing for APs (Устройство, зондирующее точки доступа)

Обычно используемые инструменты сканирования: NetStumbler (новые версии), MiniStumbler (новые версии), MACStumbler, WaveStumbler, PrismStumbler, dStumbler, iStumbler, Aerosol, Boingo™ Scans, WiNc™, AP Hopper, NetChaser.

Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer обнаруживает беспроводные устройства, зондирующие сеть WLAN и пытающиеся установить соединение (то есть передающие запрос соединения с точкой доступа с любым идентификатором SSID). Такие устройства могут представлять потенциальную угрозу безопасности одним из двух следующих способов:

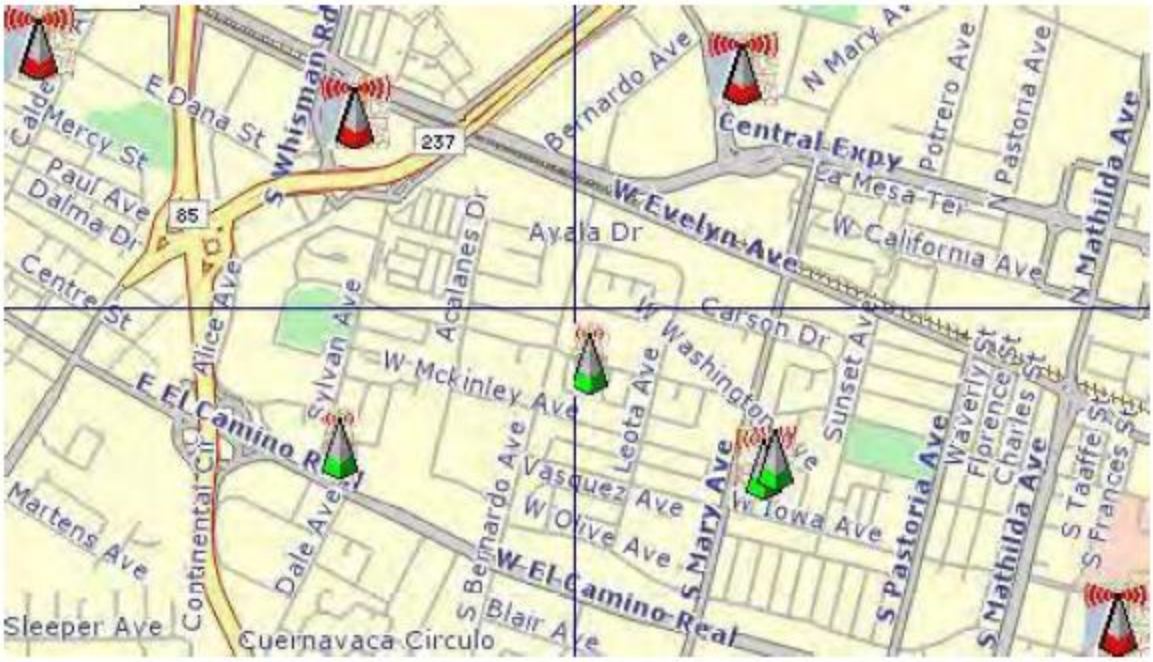
- War-driving (передвижение на автомобиле в поиске бесплатных беспроводных сетей), WiLDing (обнаружение беспроводной локальной сети), war-chalking (нанесение меток на стены и тротуары, обозначающих ближайшие бесплатные беспроводные сети), war-walking (поиск бесплатных беспроводных сетей пешком), war-cycling (передвижение на велосипеде в поиске бесплатных беспроводных сетей), war-lightrailing (передвижение на монорельсовом/узкоколейном городском транспорте в поиске бесплатных беспроводных сетей), war-busing (передвижение на автобусе в поиске бесплатных беспроводных сетей) и war-flying (полеты в поиске бесплатных беспроводных сетей).
- Легитимный беспроводной клиент пытается установить опасное беспорядочное соединение.



С помощью этих универсальных символов злоумышленник (war-chalker) обнародует обнаруженную сеть WLAN и ее конфигурацию в районе расположения этой сети.

Первой потенциальной угрозой безопасности, на которую указывает этот сигнал тревоги приложения AirMagnet WiFi Analyzer, является наличие определенной активности в отношении сети WLAN, связанной с действиями war-driving, war-chalking, war-walking и war-flying с использованием упомянутых выше

инструментов. Пытающийся проникнуть в беспроводные сети хакер использует инструменты war-driving для обнаружения точек доступа и публикации информации о них (MAC-адреса, идентификатора SSID, реализованной безопасности и т.д.) в сети Интернет с информацией о географическом местоположении точек доступа. War-chalker'ы обнаруживают точки доступа WLAN и наносят конфигурацию WLAN в общественных местах с помощью показанных выше универсальных символов. War-walking отличается от war-driving тем, что хакер идет пешком, а не едет на машине. War-flying - это, как следует из названия, поиск беспроводных сетей с воздуха. Используется то же оборудование, но из низколетящего частного самолета с мощными антеннами. Сообщалось, что такой хакер из города Перт в Австралии во время полета получал сообщения электронной почты и сеансы Internet Relay Chat (ретранслируемого интернет-чата) с высоты 1500 футов (450 метров).



Расположение точек доступа 802.11, опубликованное в Интернете группами war-driving

Вторая потенциальная угроза безопасности для подачи этого сигнала тревоги может быть еще более разрушительной. Некоторые из подобных тревог могут исходить от законных и авторизованных беспроводных клиентов в вашей сети WLAN, которые пытаются подключиться к любой точке доступа, с которой только могут связаться, включая точку доступа вашего соседа или, что создаст более серьезный ущерб, мошенническую точку доступа. Это может быть ноутбук с Microsoft Windows со встроенной картой Wi-Fi или портативные компьютеры, использующие такие инструменты беспроводной связи, как клиентская утилита Boingo™ и клиентская утилита WiNc™. После подключения злоумышленник может получить доступ к такой клиентской станции, что приведет к серьезному нарушению безопасности. Что еще хуже, клиентская станция может даже неосознанно связать постороннюю точку доступа с проводной локальной сетью вашей компании. Типичный сценарий, например, заключается в том, что современные ноутбуки оборудованы встроенными картами Wi-Fi и в то же время могут иметь физическое сетевое подключение к проводной локальной сети вашей компании. Если на этом ноутбуке с операционной системой Windows включена служба моста Windows, ваша проводная сеть будет открыта для беспроводного подключения. Для обеспечения безопасности на всех клиентских станциях должны быть настроены определенные идентификаторы SSID, что позволит избежать соединения с неавторизованной точкой доступа. Для решения такой проблемы также следует рассмотреть возможность взаимной аутентификации, такой как 802.1x и различные методы EAP.

Приложение AirMagnet WiFi Analyzer также обнаруживает беспроводную клиентскую станцию, зондирующую сеть WLAN на предмет анонимного подключения (то есть передающую запросы соединения с точкой доступа с любым идентификатором SSID) с помощью инструмента NetStumbler. Сигнал тревоги Device probing for AP (Устройство, зондирующее точку доступа) подается, когда хакеры используют новейшие версии инструмента NetStumbler. Для более старых версий приложение AirMagnet WiFi подает сигнал тревоги NetStumbler detected (Обнаружен NetStumbler).

NetStumbler - это наиболее широко используемый инструмент для обнаружения бесплатных беспроводных сетей. Веб-сайт NetStumbler (http://www.netstumbler.com/) предлагает программное

обеспечение MiniStumbler для использования на карманных компьютерах, что избавляет злоумышленника от ношения тяжелого ноутбука. Также он поддерживает больше карт, чем Wellenreiter, еще один широко используемый инструмент сканирования. War-walker'ы любят использовать MiniStumbler и аналогичные продукты для обследования торговых центров и крупные розничных магазинов.

Решение AirMagnet

Чтобы предотвратить обнаружение ваших точек доступа подобными средствами взлома, можно настроить точки доступа своей сети так, чтобы они не транслировали свой идентификатор SSID. Генерируемую сигналом тревоги AirWISE информацию можно использовать для того, чтобы определить, какая из ваших точек доступа транслирует (объявляет) свой идентификатор SSID в сигналах маяка. Затем можно настроить свойства точки доступа таким образом, чтобы отключить функцию широковещательной передачи SSID.

AP Association Capacity Full (Возможность подключения к точке доступа исчерпана)

Описание сигнала тревоги и возможные причины

Все точки доступа сети WLAN имеют ограничение на количество клиентских станций, которые могут подключиться к ним для получения услуг беспроводной связи. Обычно такое ограничение представляет собой настраиваемое пользователем на точке доступа значение. Когда точка доступа достигнет этого предела, она больше не будет принимать запросы на подключение новых клиентов.

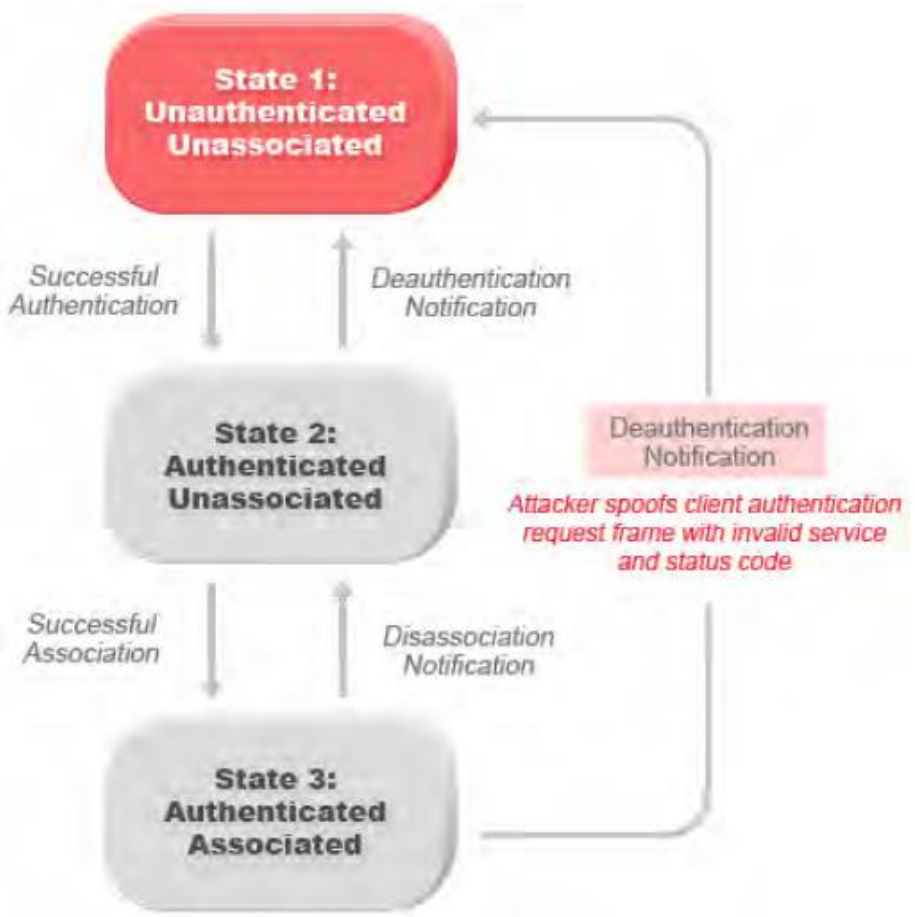
Решение AirMagnet

Для определения причины неудачных подключений приложение AirMagnet WiFi Analyzer отслеживает отклоненные запросы на подключение и ответы на них. Этот сигнал тревоги подается, если приложение AirMagnet WiFi Analyzer приходит к выводу, что отклонение связано с превышением допустимого количества соединений с точкой доступа. Данный сигнал тревоги указывает на недостаточную подготовку к развертыванию беспроводной сети или сбой балансировки нагрузки в ней. Для решения этой проблемы можно добавить к существующей инфраструктуре дополнительные точки доступа или попытаться удалить ненужные устройства, которые в настоящее время занимают соединения с текущими точками доступа.

Denial-of-Service Attack: Authentication-Failure Attack (Атака типа «отказ в обслуживании»: Атака с ошибкой аутентификации)

Описание сигнала тревоги и возможные причины

Для отслеживания аутентификации станции и проверки статуса ее подключения IEEE 802.11 задает машину состояний клиента. Беспроводные клиенты и точки доступа реализуют такую машину состояний (смотрите рисунок ниже) на основе стандарта IEEE. Успешно подключенная клиентская станция для продолжения беспроводной связи должна оставаться в Состоянии 3. Клиентская станция в Состоянии 1 или Состоянии 2 не может участвовать в процессе передачи данных по сети WLAN до тех пор, пока она не будет аутентифицирована и подключена для достижения Состояния 3. Стандарт IEEE 802.11 также задает две службы аутентификации: Open System Authentication (Открытая системная аутентификация) и Shared Key Authentication (Аутентификация с совместно используемым ключом). Для установления связи с точкой доступа беспроводные клиенты проходят один из двух процессов аутентификации.



State 1: …	Состояние 1: Аутентификация не пройдена, нет соединения
Successful Authentication	Успешная аутентификация
Deauthentication Notification	Извещение о деаутентификации
State 2:…	Состояние 2: Аутентификация пройдена, нет соединения
Attacker spoofs client authentication request…	Злоумышленник фабрикует кадр запроса аутентификации клиента с неверным кодом службы и состояния
Successful Association	Успешное подключение
Diassociation Notification	Извещение о разъединении
State 3:…	Состояние 3: Аутентификация пройдена, соединение установлено

Злоумышленник фабрикует недействительные запросы аутентификации от подключенной клиентской станции, чтобы обманом заставить точку доступа выполнить разъединение подключенного клиента.

Данная форма DoS-атаки (атаки типа «отказ в обслуживании») подделывает недопустимые кадры запроса аутентификации (с плохими кодами службы или состояния аутентификации) от подключенного клиента, находящегося в Состоянии 3 к точке доступа. После получения недействительных запросов аутентификации точка доступа изменяет статус клиента до состояния 1, что приводит к его отключению от беспроводной службы.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает эту форму атаки «отказ в обслуживании», отслеживая поддельные MAC-адреса и ошибки аутентификации. Этот сигнал тревоги также может указывать на попытку проникновения. Когда беспроводный клиент слишком много раз терпит неудачу при аутентификации соединения с точкой доступа, приложение AirMagnet WiFi Analyzer выдает этот сигнал тревоги, указывая на попытку потенциального злоумышленника взломать систему безопасности с помощью грубых компьютерных возможностей.

Примечание: Этот сигнал тревоги касается методов аутентификации 802.11 (открытая система, совместно используемый ключ и т.д.). Аутентификация на основе 802.1x и EAP отслеживается другими сигналами тревоги приложения AirMagnet WiFi Analyzer.

AP Configuration Changed (Channel) (Изменена конфигурация точки доступа (канал))

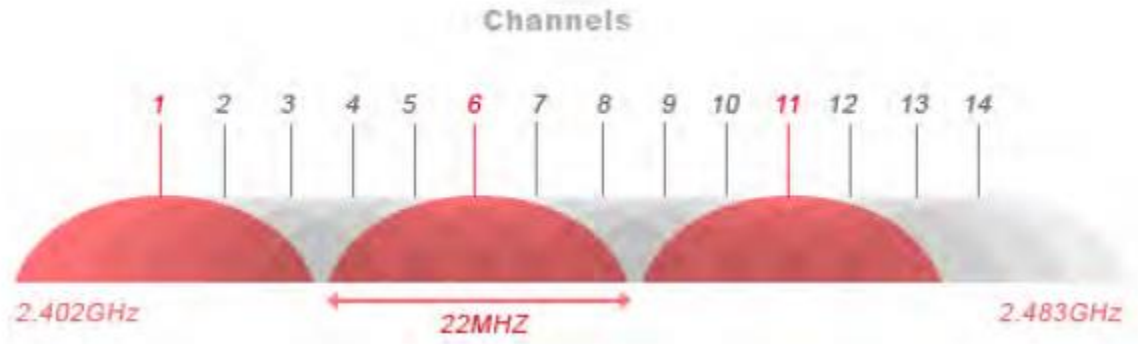
Описание сигнала тревоги и возможные причины

Большая часть современного оборудования для беспроводных локальных сетей стандарта 802.11b для передачи и получения данных использует технологию расширения спектра по методу прямой последовательности (DSSS). В технологии DSSS сигнал данных комбинируется с кодом разделения, который делит сигнал в зависимости от коэффициента расширения. Устройства 802.11a/g используют технологию OFDM (ортогональное частотное разделение каналов) для достижения более высоких скоростей передачи данных. В этой технологии высокоскоростной сигнал делится на отдельные сигналы поднесущей.
В соответствии со стандартом 802.11 канал для точки доступа устанавливает пользователь, а беспроводной клиент настраивает свою частоту на тот же канал, а затем переходит к этапу соединения.
Стандарт IEEE 802.11 требует использовать устройства 802.11b/g только в диапазоне ISM (промышленный, научный и медицинский) 2,4 ГГц, в то время как устройства 802.11a работают в диапазоне 5 ГГц UNII (нелицензируемая национальная информационная инфраструктура). Устройства 802.11a не могут взаимодействовать с устройствами 802.11b/g, поскольку они работают в разных частотных диапазонах.

Идентификатор канала	Частота в МГц	Регулятивный домен			
		Америка (-A)	Япония (-J)	Сингапур (-S)	Тайвань (-T)
34	5170	-	X	-	-
36	5180	X	-	X	-
38	5190	-	X	-	-
40	5200	X	-	X	-
42	5210	-	X	-	-
44	5220	X	-	X	-
46	5230	-	X	-	-
48	5240	X	-	X	-
52	5260	X	-	-	X
56	5280	X	-	-	X
60	5300	X	-	-	X
64	5320	X	-	-	X
149	5745	-	-	-	-
153	5765	-	-	-	-
157	5785	-	-	-	-
161	5805	-	-	-	-

Назначение каналов для устройств 802.11b. Мексика входит в домен Северной и Южной Америки, но каналы с 1 по 8 предназначены только для использования внутри помещений, а каналы с 9 по 11 можно использовать в помещении и на улице. Франция включена в регулятивный домен EMEA, но во Франции можно использовать только каналы с 10 по 13.

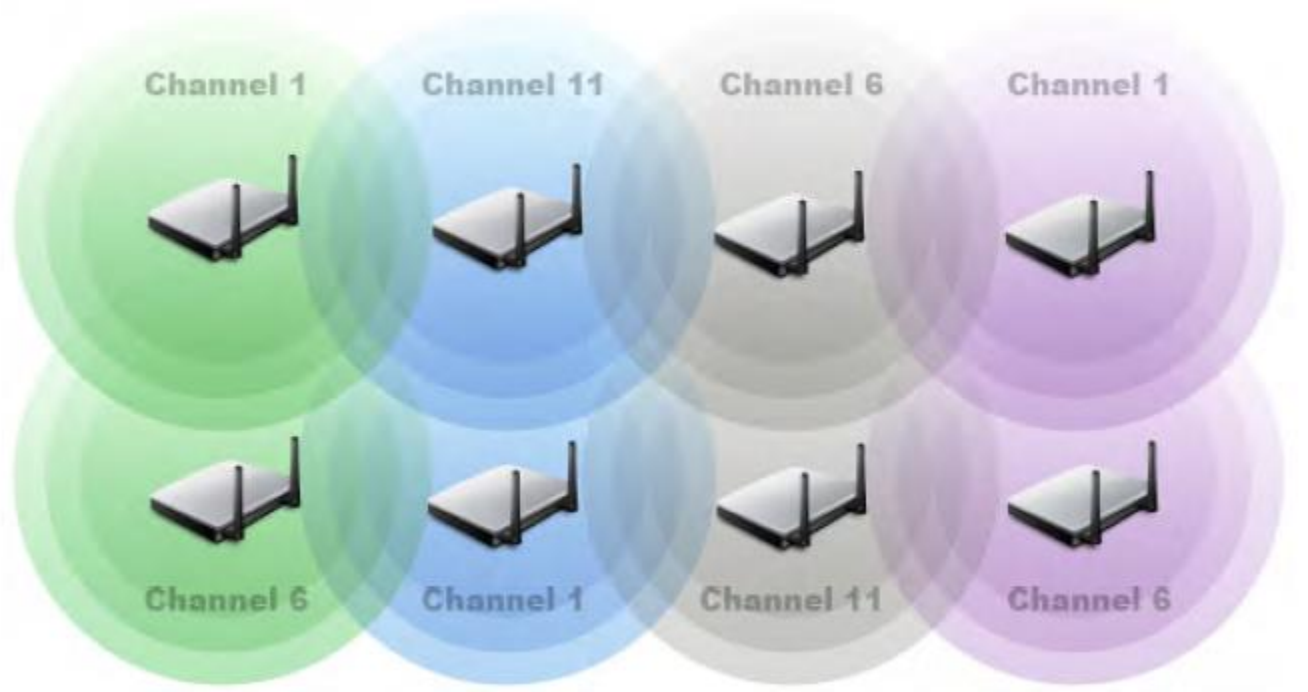
Для 802.11b/g в диапазоне ISM стандартом IEEE определено в общей сложности 14 каналов, каждый из которых занимает 22 МГц. Соседние каналы перекрываются друг с другом по используемым радиочастотам (смотрите рисунок ниже).



Channels	Каналы
2.402 GHz	2,402 ГГц
22 MHz	22 МГц
2.483 GHz	2,483 ГГц

Распределение каналов и перекрывание частот для 802.11b и 11g

Используемые беспроводными устройствами, работающими в соседних каналах (каналы отстоят друг от друга меньше, чем на пять каналов), радиочастотные полосы перекрываются, и они создают помехи друг другу. В идеальном случае для избежания подобных проблем точки доступа должны отстоять друг от друга на 5 каналов. Это означает, что в частотном спектре имеется три неперекрывающихся канала 1, 6 и 11. На рисунке ниже приводится пример распределения каналов и развертывания точки доступа.



Channel	Канал

Обследование площадки для выделения неперекрывающихся каналов физически смежным точкам доступа

После первоначального обследования площадки, в котором рассматривались каналы для различных точек доступа, очень важно не вносить никакие изменения в распределение каналов. Любые изменения могут привести к потенциальным помехам между точками доступа и увеличению уровня шумов в частотном спектре. Такое изменение может сделать бесполезным предварительное и последующее обследования площадки. Внезапные изменения распределения каналов для точек доступа могут также указывать на то, что доступ к точке доступа получил посторонний, который и внес эти изменения.

Решение AirMagnet

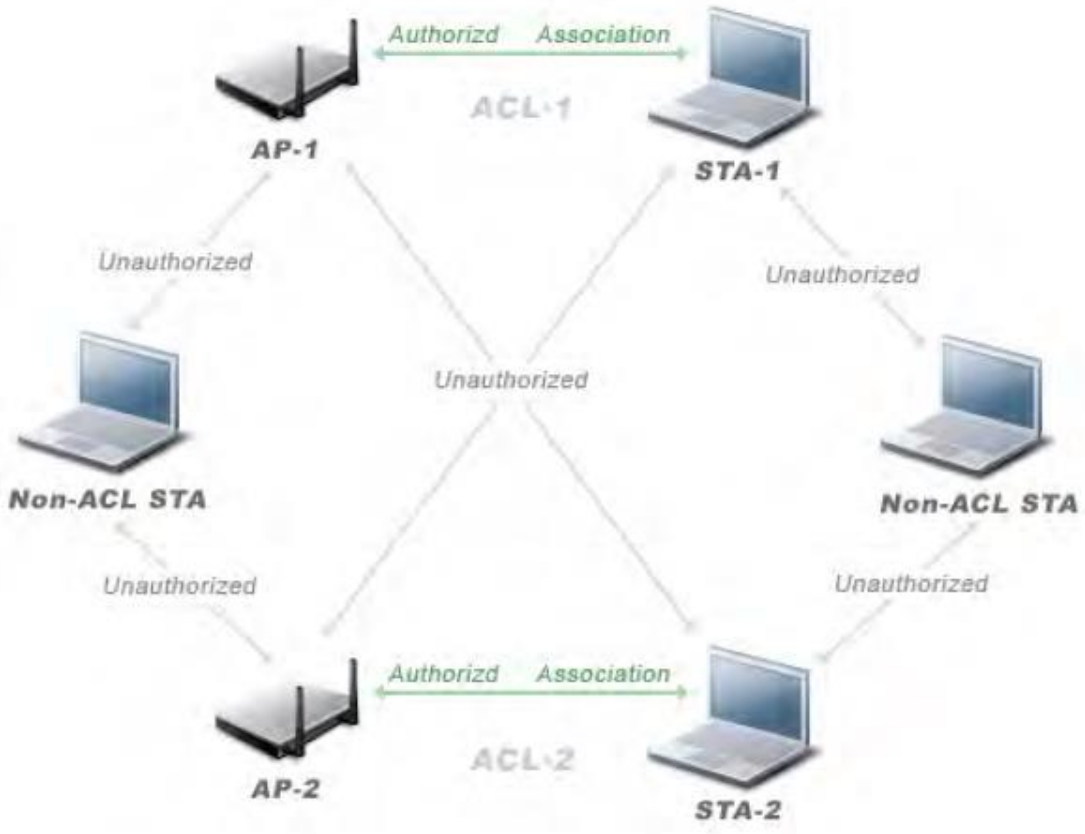
Приложение AirMagnet WiFi Analyzer также предупреждает о любых внезапных изменениях идентификатора SSID точки доступа. Это может указывать на то, что злоумышленник контролирует точку доступа и изменил конфигурацию SSID, что способно привести к отключению всех легитимных клиентов от точки доступа, поскольку теперь они не общаются в одной сети. Чтобы продолжить предоставление услуг клиентам, подключитесь к точке доступа, конфигурация которой изменилась, назначьте более надежный пароль для входа в систему и измените идентификатор SSID обратно на исходный.

Unauthorized Association Detected (Обнаружено неавторизованное подключение)

Описание сигнала тревоги и возможные причины

Соединением точки доступа со станцией в корпоративной сети WLAN можно управлять с помощью списка контроля доступа к сети (ACL), который состоит из MAC-адресов всех точек доступа и станций, официально развернутых в сети. Список ACL указывает, что точки доступа могут связываться только со станциями из того же списка ACL, и наоборот. Любая связь точки доступа со станцией за пределами списка ACL является неавторизованной и, следовательно, запрещена. После настройки в приложении AirMagnet Wi-Fi Analyzer список ACL можно использовать в качестве эффективного инструмента обнаружения и предупреждения администраторов WLAN о любых неавторизованных соединениях, происходящих на сети WLAN. Ниже приведены типичные ситуации неавторизованных соединений, которые также показаны на следующей диаграмме:

- Точка доступа из одного списка ACL связывается со станцией из другого списка ACL, или наоборот.
- Станция, включенная в список ACL, связывается с точкой доступа, не включенной ни в какой список ACL.
- Точка доступа, включенная в список ACL, связывается со станцией, не включенной ни в какой список ACL.



Authorized Association	Авторизованное соединение
Unauthorized	Неавторизованное
Non-ACL STA	Станция, не входящая в список ACL

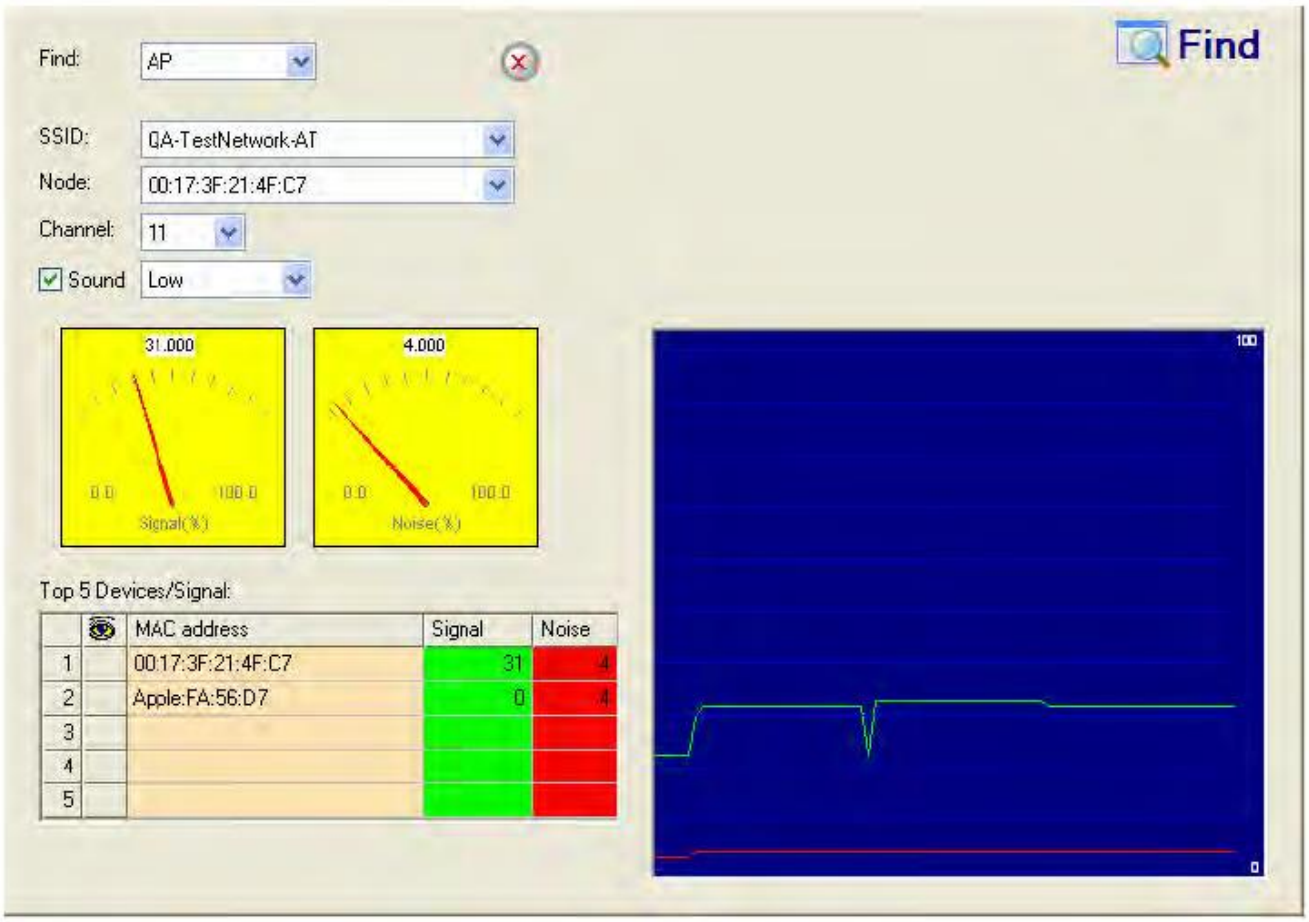
На приведенной выше диаграмме показаны три сценария неавторизованных соединений точки доступа и станции, показанных красными стрелками. Обратите внимание, что к точкам доступа/станциям, не входящим в список ACL, относятся все точки доступа или станции, которые не входят в ACL, в том числе неавторизованные точки доступа и станции, точки доступа и станции соседних сетей, гостевые точки доступа и станции и т.д. Кроме того, авторизованное соединение точки доступа и станции может устанавливаться только между точками доступа и станциями из одного списка ACL.

В корпоративной сетевой среде устанавливаемые сотрудниками неавторизованные точки доступа обычно не соответствуют стандартной практике развертывания сети и, следовательно, нарушают ее целостность. Они представляют собой лазейки в сетевой безопасности и позволяют злоумышленникам легко взломать проводную сеть предприятия. В настоящее время одной из основных проблем, с которыми сталкивается большинство администраторов беспроводных сетей, является неавторизованные соединения между станциями, входящими в список ACL, и неавторизованной точкой доступа. Поскольку данные, передаваемые на станции и от них, проходят через неавторизованную точку доступа, хакеры способны получить доступ к любой конфиденциальной информации. С другой стороны, неавторизованные станции не только вызывают проблемы с безопасностью, но и снижают производительность сети. Они работают в эфире и конкурируют за пропускную способность сети с авторизованными клиентами. Поскольку точка доступа способна обслуживать только определенное количество станций, она начнет отклонять запросы на соединение от станций, как только будет достигнуто предельное количество подключений. Загруженная мошенническими станциями точка доступа будет отказывать легитимным станциям в доступе к сети. К наиболее частым проблемам, создаваемым неавторизованными станциями, относятся разрыв соединений и снижение производительности сети.

Пользователи могут использовать экран Start приложения AirMagnet WiFi Analyzer, чтобы сделать все легитимные устройства своей сети допустимыми, щелкнув правой кнопкой мыши по экрану и выбрав категорию Valid Device (Допустимое устройство) в контекстном меню. При этом приложение будет рассматривать все неизвестные устройства как мошеннические и, следовательно, инициировать этот сигнал тревоги, если в сети будет обнаружено неизвестное устройство.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer с помощью этого сигнала тревоги может автоматически предупреждать сетевых администраторов о любом обнаруженном в сети неавторизованном соединении точки доступа со станцией. После появления сигнала тревоги необходимо идентифицировать мошенническое или неавторизованное устройство и предпринять действия для решения данной проблемы. Используйте инструмент поиска Find приложения AirMagnet WiFi Analyzer, чтобы физически найти точку доступа и станцию, вовлеченные в неавторизованное соединение. Выведите их из эксплуатации, чтобы предотвратить дальнейшее нарушение безопасности сети.

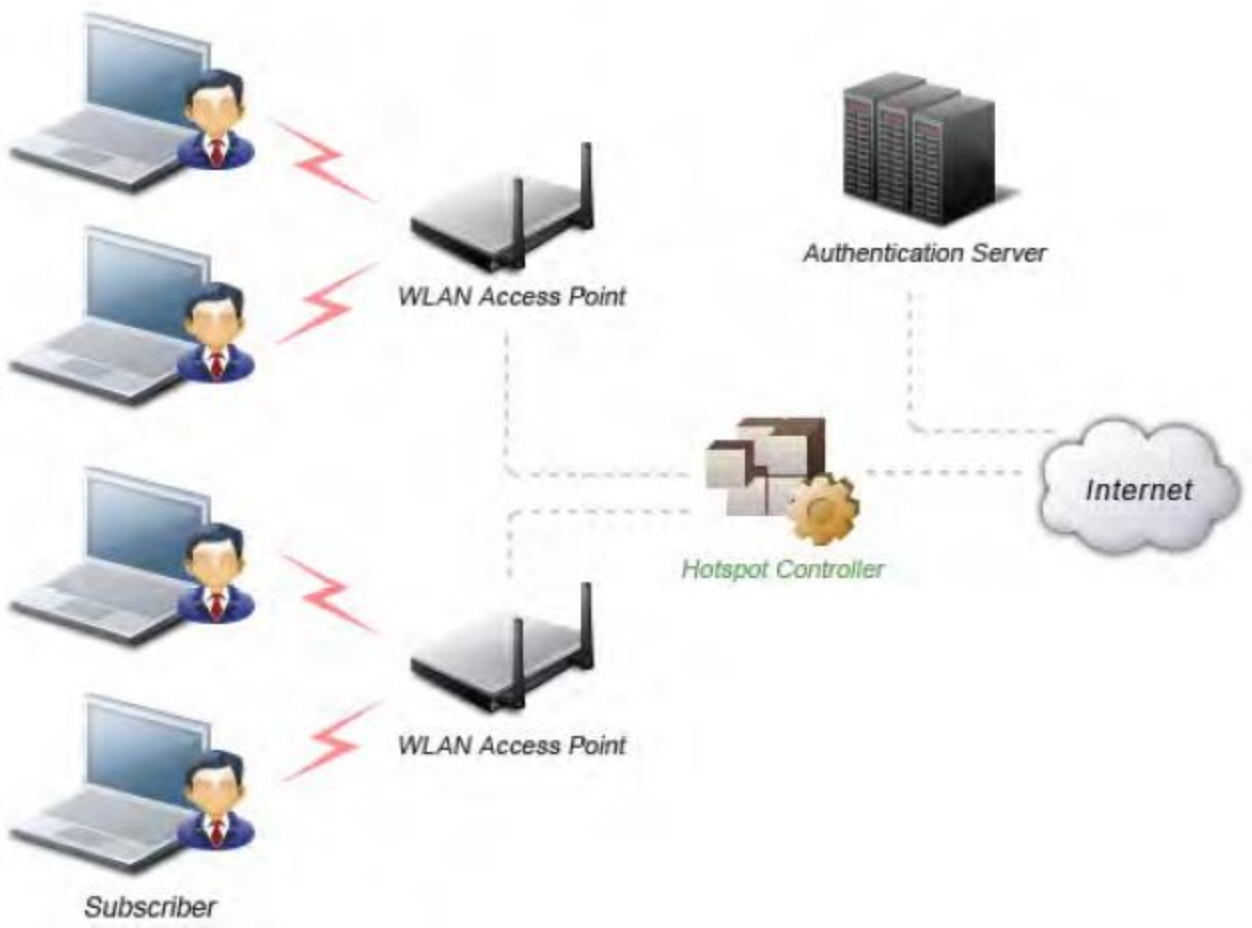


Инструмент поиска Find приложения AirMagnet WiFi Analyzer находит устройство, отслеживая его сигнал и уровень шума.

Airsnarf Attack Detected (Обнаружена атака Airsnarf)

Описание сигнала тревоги и возможные причины

Публичная точка доступа - это любое место, где доступ к сети Wi-Fi предоставляется широкой публике. Подобные точки доступа часто встречаются в аэропортах, отелях, кафе и других местах, где обычно собираются деловые люди. В наши дни это, вероятно, одна из самых важных услуг доступа к сети для деловых путешественников. Все, что требуется клиенту, это иметь ноутбук или карманное устройство с поддержкой беспроводной связи. Затем пользователь может подключиться к легитимной точке доступа и получить услугу. Большинство публичных точек доступа не требуют для подключения от пользователя какого-либо расширенного механизма аутентификации, кроме всплывающего окна веб-страницы для входа пользователя. Таким образом, критерий входа зависит только от того, оплатил ли подписчик абонентскую плату или нет. О среде публичных беспроводных точек доступа можно сказать, что здесь никому нельзя доверять. В наши дни по соображениям безопасности некоторые производители публичных точек доступа WLAN используют для проверки личности пользователя механизмы аутентификации 802.1x или выше.



WLAN Access Point	Точка доступа к беспроводной локальной сети
Authentication Server	Сервер аутентификации
Hotspot Controller	Контроллер публичной точки доступа
Internet	Интернет
Subscriber	Подписчик

Основные компоненты сети WLAN с публичной точкой доступа

Четырьмя компонентами базовой сети с публичной точкой доступа являются:

- Подписчики публичной точки доступа: Это легитимные пользователи с ноутбуком или портативным устройством с поддержкой беспроводной связи и действующим логином для доступа к сети с публичной точкой доступа.
- Точки доступа WLAN: В зависимости от реализации сети с публичной точкой доступа это могут быть шлюзы SOHO или точки доступа корпоративного уровня.
- Контроллеры публичных точек доступа: Этот компонент имеет дело с аутентификацией пользователя, сбором информации для выставления счетов, отслеживанием времени использования, функциями фильтрации и т.д. Это может быть независимый компьютер или контроллер, встроенный в саму точку доступа.
- Сервер аутентификации: Этот сервер содержит учетные данные подписчиков. Контроллер публичной точки доступа в большинстве случаев после получения учетных данных подписчиков проверяет их на сервере аутентификации.

Airsnarf - это утилита для настройки точки беспроводного доступа, показывающая, как хакер может украсть учетные данные пользователя (имя и пароль) из общедоступных точек беспроводного доступа.

Основанный на скриптах оболочки инструмент Airsnarf создает публичную точку доступа с адаптивным порталом, куда пользователи вводят свои данные для входа. В файле конфигурации airsnarf можно настроить такие важные параметры, как информация о локальной сети, IP-адрес шлюза и SSID. Этот инструмент изначально передает очень сильный сигнал, который отсоединяет беспроводных клиентов публичной точки доступа от авторизованной точки доступа, обеспечивающей доступ в сеть Интернет. Беспроводные клиенты, предполагающие, что они были просто временно отключены от сети Интернет из-

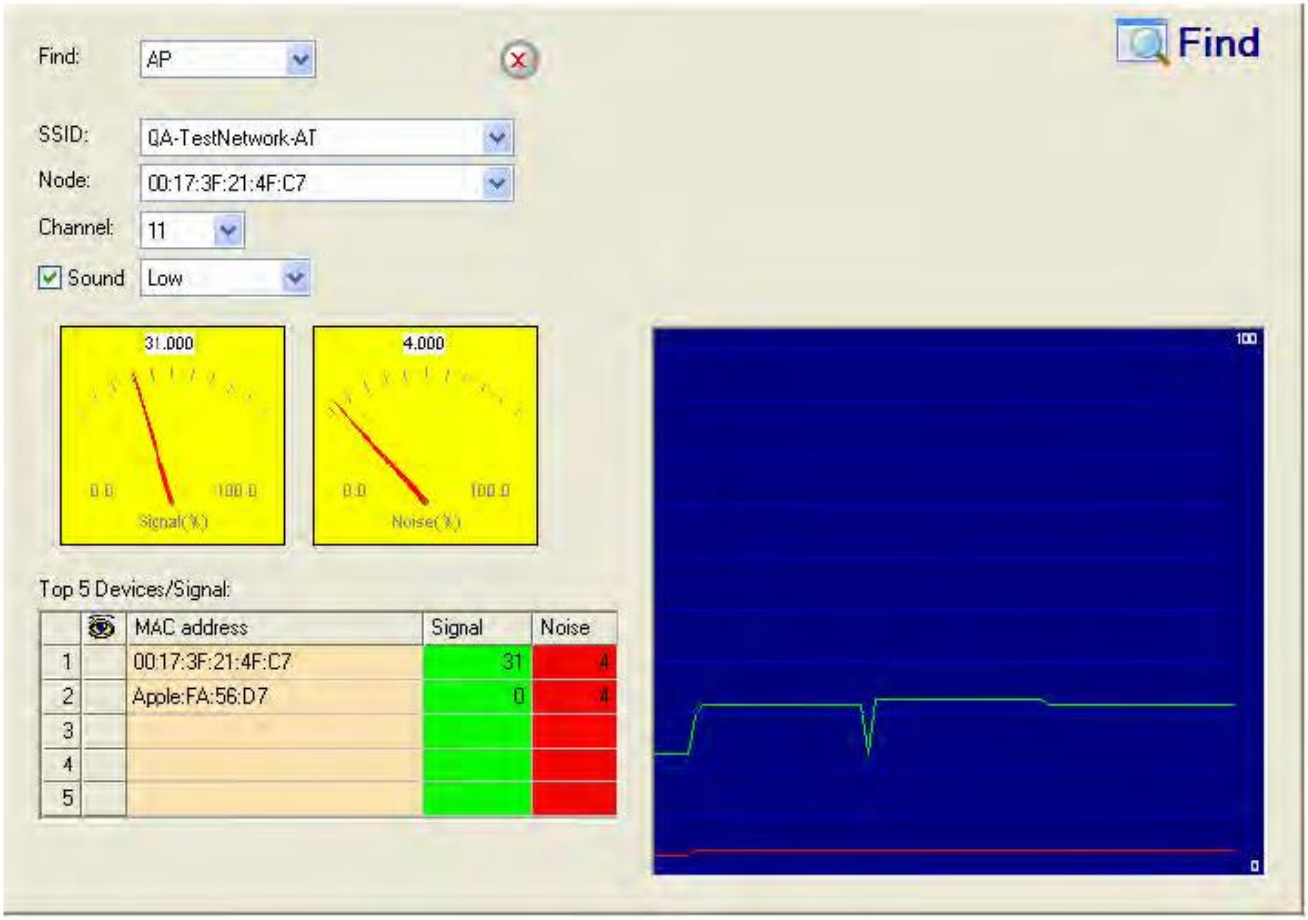
за какой-то неизвестной проблемы, попытаются снова войти в систему, чтобы возобновить свою работу. Ничего не подозревающие беспроводные клиенты, связывающиеся с точкой доступа Airsnarf, получают IP-адрес, DNS-адрес и IP-адрес шлюза от мошеннической точки доступа Airsnarf вместо легитимной точки доступа, установленной оператором публичных точек доступа. Пользователям будет показана веб-страница, запрашивающая имя пользователя и пароль, так как теперь запросы DNS решаются мошеннической точкой доступа Airsnarf. Введенные имена пользователей и пароли будут собираться хакером.

Имя пользователя и пароль можно будет использовать в любой другой точке доступа того же провайдера в любой точке страны, при этом пользователь не будет осознавать их мошенническое использование. Единственный случай, когда это может иметь небольшие последствия, это если пользователь точки доступа подключен по схеме с поминутной оплатой.

Инструмент Airsnarf также позволяет проникать в портативные компьютеры, которые неосознанно подключаются к точке доступа Airsnarf. Хакеры могут загрузить инструмент AirSnarf с http://airsnarf.shmoo.com/

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаружит беспроводное устройство, на котором запущен инструмент AirSnarf. Администратор должен предпринять соответствующие действия для удаления инструмента AirSnarf из среды WLAN. Для этого можно использовать инструмент Find (Найти).



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Potential ASLEAP Attack Detected (Обнаружена потенциальная атака ASLEAP)

Описание сигнала тревоги и возможные причины

Широко известно, что устройства WLAN, использующие для шифрования статический ключ WEP, уязвимы для атаки взлома ключа WEP (Обратитесь к документу «Weaknesses in the Key Scheduling Algorithm of RC4 – I» (Слабые стороны алгоритма планирования ключей RC4 – I), авторы Scott Fluhrer, Itsik Mantin и Adi Shamir (Скотт Флурер, Ицик Мантин и Ади Шамир)).

Для использования существующей структуры 802.1x для предотвращения подобных атак на ключ WEP компания Cisco Systems представила LEAP (Lightweight Extensible Authentication Protocol – Облегченный протокол расширенной аутентификации). Решение Cisco LEAP обеспечивает взаимную аутентификацию, динамическую для каждого сеанса и для каждого пользовательского ключа, а также настраиваемый таймаут сеансового ключа WEP. Решение LEAP считалось не только стабильным решением безопасности, но и простым в настройке.

Джошуа Райт, сетевой инженер из Johnson & Wales University в Провиденсе, Род-Айленд, написал инструмент для взлома, который компрометирует беспроводные сети LAN, использующие LEAP. В этом инструменте для взлома паролей LEAP используются автономные атаки по словарю. После обнаружения сетей WLAN, использующих LEAP, этот инструмент отменяет аутентификацию пользователей, вынуждая их подключаться повторно и предоставлять свои учетные данные (имя пользователя и пароль). Хакер получает возможность захватывать пакеты законных пользователей, пытающихся повторно получить доступ к сети. После этого злоумышленник может анализировать трафик в режиме офлайн и угадывать пароль, проверяя значения из словаря.

Основные возможности инструмента ASLEAP:
- Чтение в реальном времени с любого беспроводного интерфейса в режиме RFMON с помощью libpcap.
- Мониторинг одного канала или переключение каналов для поиска целевых сетей, в которых работает LEAP.
- Активная деаутентификация пользователей в сетях LEAP, которая заставит их аутентифицироваться повторно. Это значительно ускоряет захват паролей LEAP.
- Деаутентификация только тех пользователей, которые еще не были замечены, позволяет не тратить время на пользователей, не использующих LEAP.
- Чтение из сохраненных файлов libpcap.
- Использование динамической таблицы базы данных и индекса для очень быстрого поиска в больших файлах. Это сокращает время поиска в худшем случае до 0,0015% по сравнению с поиском в плоском (однородном) файле.
- Запись в файл libpcap только информации об обмене LEAP.

Этот инструмент можно использовать для захвата учетных данных LEAP с устройством, которому не хватает места на диске (например, iPaq), с последующей обработкой учетных данных LEAP, хранящихся в файле libpcap, в системе с большими ресурсами хранения, для проведения атаки по словарю.

Исходный код и двоичный дистрибутив Win32 для этого инструмента доступны по адресу http://asleap.sourceforge.net.

Cisco Systems разработала протокол EAP-FAST (Протокол расширенной аутентификации с гибкой аутентификацией через безопасное туннелирование), который способен остановить подобные атаки по словарю. Протокол EAP-FAST помогает предотвратить атаки типа «злоумышленник посередине», атаки по словарю, атаки с подделкой пакетов и аутентификации. В протоколе EAP-FAST между клиентом и сервером создается туннель с использованием PAC (Protected Access Credential – Защищенные учетные данные доступа) для аутентификации друг друга. После процесса установления туннеля клиент аутентифицируется с использованием учетных данных (имени пользователя и пароля).

Некоторые из основных преимуществ протокола EAP-FAST заключаются в том, что он не является проприетарным, совместим со стандартом IEEE 802.11i, поддерживает TKIP и WPA, не использует сертификаты, что позволяет избежать сложных инфраструктур PKI, и поддерживает несколько операционных систем на ПК и карманных ПК.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает наличие потенциального инструмента атаки ASLEAP. После обнаружения приложение AirMagnet WiFi Analyzer предупреждает администратора беспроводной сети, а пользователю атакуемой станции рекомендует сбросить свой пароль. Лучшим решением противодействия потенциальным атакам ASLEAP является замена протокола LEAP на протокол EAP-FAST в корпоративной среде WLAN.

RF Regulatory Rule Violation (Нарушение нормативных правил в области радиочастот)

Описание сигнала тревоги и возможные причины

Большая часть современного оборудования для беспроводных локальных сетей стандарта 802.11b для передачи и получения данных использует технологию расширения спектра по методу прямой последовательности (DSSS). В технологии DSSS сигнал данных комбинируется с кодом разделения, который делит сигнал в зависимости от коэффициента расширения. Устройства 802.11a/g используют технологию OFDM (ортогональное частотное разделение каналов) для достижения более высоких скоростей передачи данных. В этой технологии высокоскоростной сигнал делится на отдельные сигналы поднесущей.

Стандарт IEEE 802.11 требует использовать устройства 802.11b/g только в диапазоне ISM (промышленный, научный и медицинский) 2,4 ГГц, в то время как устройства 802.11a работают в диапазоне 5 ГГц UNII (нелицензируемая национальная информационная инфраструктура). Устройства 802.11a не могут взаимодействовать с устройствами 802.11b/g, поскольку они работают в разных частотных диапазонах. В соответствии со стандартом 802.11 канал для точки доступа устанавливает пользователь, а беспроводной клиент настраивает свою частоту на тот же канал, а затем переходит к этапу соединения.

В каждом регионе имеется свой собственный местный регулирующий орган, который контролирует работу устройств 802.11, гарантируя, что они работают в правильном канале. В США этим регулирующим органом является Федеральная комиссия связи (FCC). Для устройств 802.11b/g в США FCC разрешает безлицензионное использование только 11 каналов. Любое устройство, работающее на других частотах, нарушает правила, что может повлечь за собой строгие меры со стороны государственного органа.

Идентификатор канала	Частота в МГц	Регулятивный домен			
		Америка (-A)	Япония (-J)	Сингапур (-S)	Тайвань (-T)
34	5170	-	X	-	-
36	5180	X	-	X	-
38	5190	-	X	-	-
40	5200	X	-	X	-
42	5210	-	X	-	-
44	5220	X	-	X	-
46	5230	-	X	-	-
48	5240	X	-	X	-
52	5260	X	-	-	X
56	5280	X	-	-	X
60	5300	X	-	-	X
64	5320	X	-	-	X
149	5745	-	-	-	-
153	5765	-	-	-	-
157	5785	-	-	-	-
161	5805	-	-	-	-

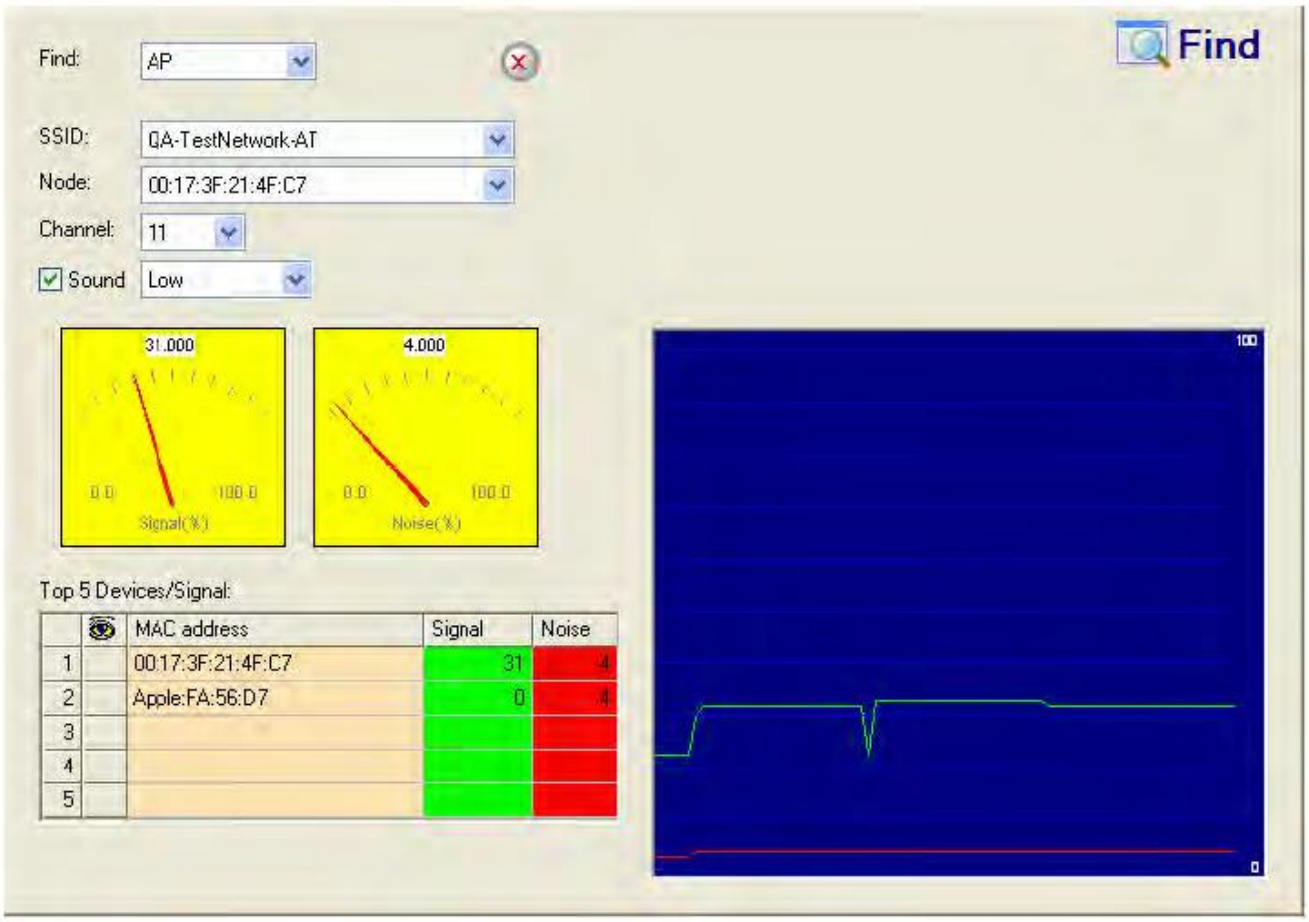
Назначение каналов для устройств 802.11a. Все каналы предназначены для использования в помещении, за исключением каналов с 52 по 64 в Северной и Южной Америке, которые можно использовать в помещении и на улице.

Идентификатор канала	Частота в МГц	Регулятивный домен				
		Америка (-A)	EMEA (-E)	Израиль (-I)	Китай (-C)	Япония (-J)
1	2412	X	X	-	X	X
2	2417	X	X	-	X	X
3	2422	X	X	X	X	X
4	2427	X	X	X	X	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X
8	2447	X	X	X	X	X
9	2452	X	X	X	X	X
10	2457	X	X	-	X	X
11	2462	X	X	-	X	X
12	2467	-	X	-	-	X
13	2472	-	X	-	-	X
14	2484	-	-	-	-	X

Назначение каналов для устройств 802.11b. Мексика входит в домен Северной и Южной Америки, но каналы с 1 по 8 предназначены только для использования внутри помещений, а каналы с 9 по 11 можно использовать в помещении и на улице. Франция включена в регулятивный домен EMEA, но во Франции можно использовать только каналы с 10 по 13.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает устройства 802.11, работающие на каналах, которые не разрешены для использования местным регулирующим органом. Например, в США приложение AirMagnet WiFi Analyzer способно обнаружить точку доступа, работающую на канале 14, что является нарушением, поскольку FCC не авторизовала этот канал для использования. Администратор должен предпринять соответствующие шаги, чтобы найти устройство и удалить его из беспроводной среды. После того, как нарушившая точка доступа идентифицирована и информация о ней получена из приложения AirMagnet WiFi Analyzer, администратор WLAN может использовать инструмент FIND (Найти) для определения местоположения устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Device Unprotected by EAP-FAST (Устройство не защищено протоколом EAP-FAST)

Описание сигнала тревоги и возможные причины

Широко известно, что устройства WLAN, использующие для шифрования статический ключ WEP, уязвимы для атаки взлома ключа WEP (Обратитесь к документу «Weaknesses in the Key Scheduling Algorithm of RC4 – I» (Слабые стороны алгоритма планирования ключей RC4 – I), авторы Scott Fluhrer, Itsik Mantin и Adi Shamir (Скотт Флурер, Ицик Мантин и Ади Шамир)).

Для использования существующей структуры 802.1x для предотвращения таких атак на ключ WEP компания Cisco Systems представила LEAP (Lightweight Extensible Authentication Protocol – Облегченный протокол расширенной аутентификации). Решение Cisco LEAP обеспечивает взаимную аутентификацию, динамическую для каждого сеанса и для каждого пользовательского ключа, а также настраиваемый таймаут сеансового ключа WEP. Решение LEAP считалось не только стабильным решением безопасности, но и простым в настройке.

Джошуа Райт, сетевой инженер из Johnson & Wales University в Провиденсе, Род-Айленд, написал инструмент для взлома, который компрометирует беспроводные сети LAN, использующие LEAP. В этом инструменте для взлома паролей LEAP используются автономные атаки по словарю. После обнаружения сетей WLAN, использующих LEAP, этот инструмент отменяет аутентификацию пользователей, вынуждая их подключаться повторно и предоставлять свои учетные данные (имя пользователя и пароль). Хакер получает возможность захвата пакетов легитимных пользователей, пытающихся повторно получить доступ к сети. После этого злоумышленник может анализировать трафик в режиме офлайн и угадывать пароль, проверяя значения из словаря.

Основные возможности инструмента ASLEAP:

- Чтение в реальном времени с любого беспроводного интерфейса в режиме RFMON с помощью libpcap.
- Мониторинг одного канала или переключение каналов для поиска целевых сетей, в которых работает LEAP.
- Активная деаутентификация пользователей в сетях LEAP, которая заставит их аутентифицироваться повторно. Это значительно ускоряет захват паролей LEAP.
- Деаутентификация только тех пользователей, которые еще не были замечены, позволяет не тратить время на пользователей, не использующих LEAP.
- Чтение из сохраненных файлов libpcap.
- Использование динамической таблицы базы данных и индекса для очень быстрого поиска в больших файлах. Это сокращает время поиска в худшем случае до 0,0015% по сравнению с поиском в плоском (однородном) файле.
- Запись в файл libpcap только информации об обмене LEAP.

Этот инструмент можно использовать для захвата учетных данных LEAP с устройством, которому не хватает места на диске (например, iPaq), с последующей обработкой учетных данных LEAP, хранящихся в файле libpcap, в системе с большими ресурсами хранения, для проведения атаки по словарю.

Исходный код и двоичный дистрибутив Win32 для этого инструмента доступны по адресу http://asleap.sourceforge.net.

Cisco Systems разработала протокол EAP-FAST (Протокол расширенной аутентификации с гибкой аутентификацией через безопасное туннелирование), который способен остановить подобные атаки по словарю. Протокол EAP-FAST помогает предотвратить атаки типа «злоумышленник посередине», атаки по словарю, атаки с подделкой пакетов и аутентификации. В протоколе EAP-FAST между клиентом и сервером создается туннель с использованием PAC (Protected Access Credential – Защищенные учетные данные доступа) для аутентификации друг друга. После процесса установления туннеля клиент аутентифицируется с использованием учетных данных (имени пользователя и пароля).

Некоторые из основных преимуществ протокола EAP-FAST заключаются в том, что он не является проприетарным, совместим со стандартом IEEE 802.11i, поддерживает TKIP и WPA, не использует сертификаты, что позволяет избежать сложных инфраструктур PKI и поддерживает несколько операционных систем на ПК и карманных ПК.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer предупреждает администратора беспроводной сети об устройствах, которые используют механизм аутентификации 802.1x, но не используют протокол EAP-FAST. Рекомендуется внедрить протокол EAP-FAST в беспроводную среду.

LEAP Vulnerability Detected (Обнаружена уязвимость LEAP)

Описание сигнала тревоги и возможные причины

Широко известно, что устройства WLAN, использующие для шифрования статический ключ WEP, уязвимы для атаки взлома ключа WEP (Обратитесь к документу «Weaknesses in the Key Scheduling Algorithm of RC4 – I» (Слабые стороны алгоритма планирования ключей RC4 – I), авторы Scott Fluhrer, Itsik Mantin и Adi Shamir (Скотт Флурер, Ицик Мантин и Ади Шамир)).

Для использования существующей структуры 802.1x для предотвращения таких атак на ключ WEP компания Cisco Systems представила LEAP (Lightweight Extensible Authentication Protocol – Облегченный протокол расширенной аутентификации). Решение Cisco LEAP обеспечивает взаимную аутентификацию, динамическую для каждого сеанса и для каждого пользовательского ключа, а также настраиваемый таймаут сеансового ключа WEP. Решение LEAP считалось не только стабильным решением безопасности, но и простым в настройке.

Джошуа Райт, сетевой инженер из Johnson & Wales University в Провиденсе, Род-Айленд, написал инструмент для взлома, который компрометирует беспроводные сети LAN, использующие LEAP. В этом инструменте для взлома паролей LEAP используются автономные атаки по словарю. После обнаружения сетей WLAN, использующих LEAP, этот инструмент отменяет аутентификацию пользователей, вынуждая их подключаться повторно и предоставлять свои учетные данные (имя пользователя и пароль). Хакер

получает возможность захватывать пакеты законных пользователей, пытающихся повторно получить доступ к сети. После этого злоумышленник может анализировать трафик в режиме офлайн и угадывать пароль, проверяя значения из словаря.

Основные возможности инструмента ASLEAP:
- Чтение в реальном времени с любого беспроводного интерфейса в режиме RFMON с помощью libpcap.
- Мониторинг одного канала или переключение каналов для поиска целевых сетей, в которых работает LEAP.
- Активная деаутентификация пользователей в сетях LEAP, которая заставит их аутентифицироваться повторно. Это значительно ускоряет захват паролей LEAP.
- Деаутентификация только тех пользователей, которые еще не были замечены, позволяет не тратить время на пользователей, не использующих LEAP.
- Чтение из сохраненных файлов libpcap.
- Использование динамической таблицы базы данных и индекса для очень быстрого поиска в больших файлах. Это сокращает время поиска в худшем случае до 0,0015% по сравнению с поиском в плоском (однородном) файле.
- Запись в файл libpcap только информации об обмене LEAP.

Это можно использовать для захвата учетных данных LEAP с устройством, которому не хватает места на диске (например, iPaq), с последующей обработкой учетных данных LEAP, хранящихся в файле libpcap, в системе с большими ресурсами хранения, для проведения атаки по словарю.

Исходный код и двоичный дистрибутив Win32 для этого инструмента доступны по адресу http://asleap.sourceforge.net.

Cisco Systems разработала протокол EAP-FAST (Протокол расширенной аутентификации с гибкой аутентификацией через безопасное туннелирование), который способен остановить подобные атаки по словарю. Протокол EAP-FAST помогает предотвратить атаки типа «злоумышленник посередине», атаки по словарю, атаки с подделкой пакетов и аутентификации. В протоколе EAP-FAST между клиентом и сервером создается туннель с использованием PAC (Protected Access Credential – Защищенные учетные данные доступа) для аутентификации друг друга. После процесса установления туннеля клиент аутентифицируется с использованием учетных данных (имени пользователя и пароля).

Некоторые из основных преимуществ протокола EAP-FAST заключаются в том, что он не является проприетарным, совместим со стандартом IEEE 802.11i, поддерживает TKIP и WPA, не использует сертификаты, что позволяет избежать сложных инфраструктур PKI и поддерживает несколько операционных систем на ПК и карманных ПК.

Решение AirMagnet

AirMagnet WiFi Analyzer предупреждает администратора беспроводной сети об устройствах, которые используют LEAP, уязвимы для атаки ASLEAP и рискуют раскрыть информацию об имени пользователя и пароле. Рекомендуется внедрить в беспроводную среду протокол EAP-FAST.

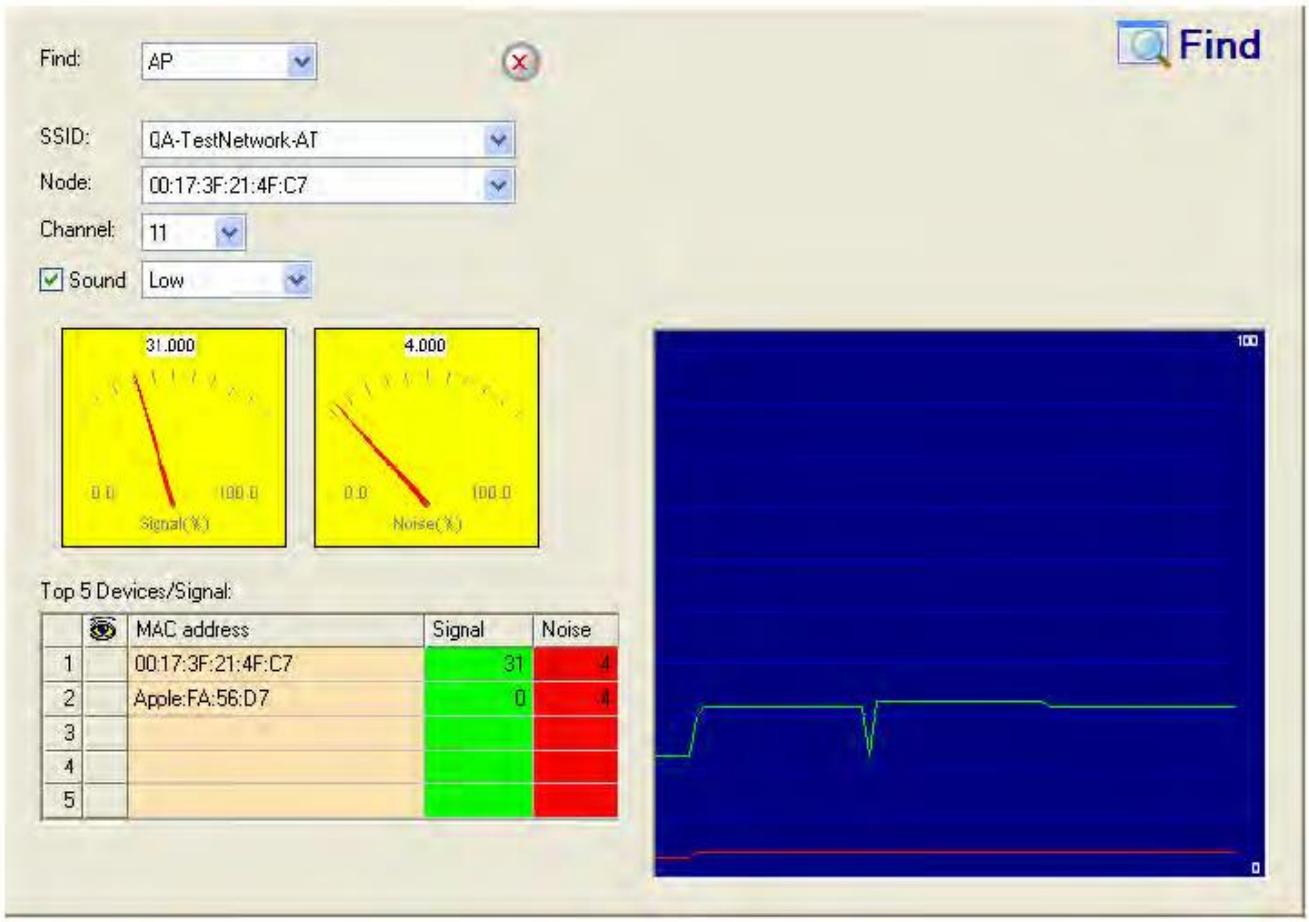
Malformed 802.11 Packets Detected (Обнаружены искаженные пакеты 802.11)

Описание сигнала тревоги и возможные причины

Хакеры, используя незаконные пакеты (искаженные нестандартные кадры 802.11), могут заставить беспроводные устройства вести себя странным образом. Хорошо известно, что незаконные пакеты могут вызывать сбой прошивки беспроводных сетевых карт некоторых производителей. Примеры такой уязвимости включают НУЛЕВОЙ кадр ответа на зондирование (нулевой идентификатор SSID в кадре ответа на зондирование) и элементы информации чрезмерно большого размера в кадрах управления. Эти неправильно сформированные кадры могут транслироваться для вызова сбоя нескольких беспроводных клиентов.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer способно обнаруживать эти незаконные пакеты и подавать сигнал тревоги при их появлении. Беспроводным клиентам, сталкивающимся во время атаки с синим экраном или испытывающим проблемы с блокировкой, следует рассмотреть возможность обновления драйвера или прошивки сетевой карты WLAN.
После того, как клиент идентифицирован и об этом сообщило приложение AirMagnet WiFi Analyzer, администратор WLAN сможет использовать инструмент FIND, чтобы найти его.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая их сигнал и шум

Denial-of-Service Attack: PS Poll Flood Attack (Атака типа «отказ в обслуживании»: Флуд-атака с использованием опроса PS)

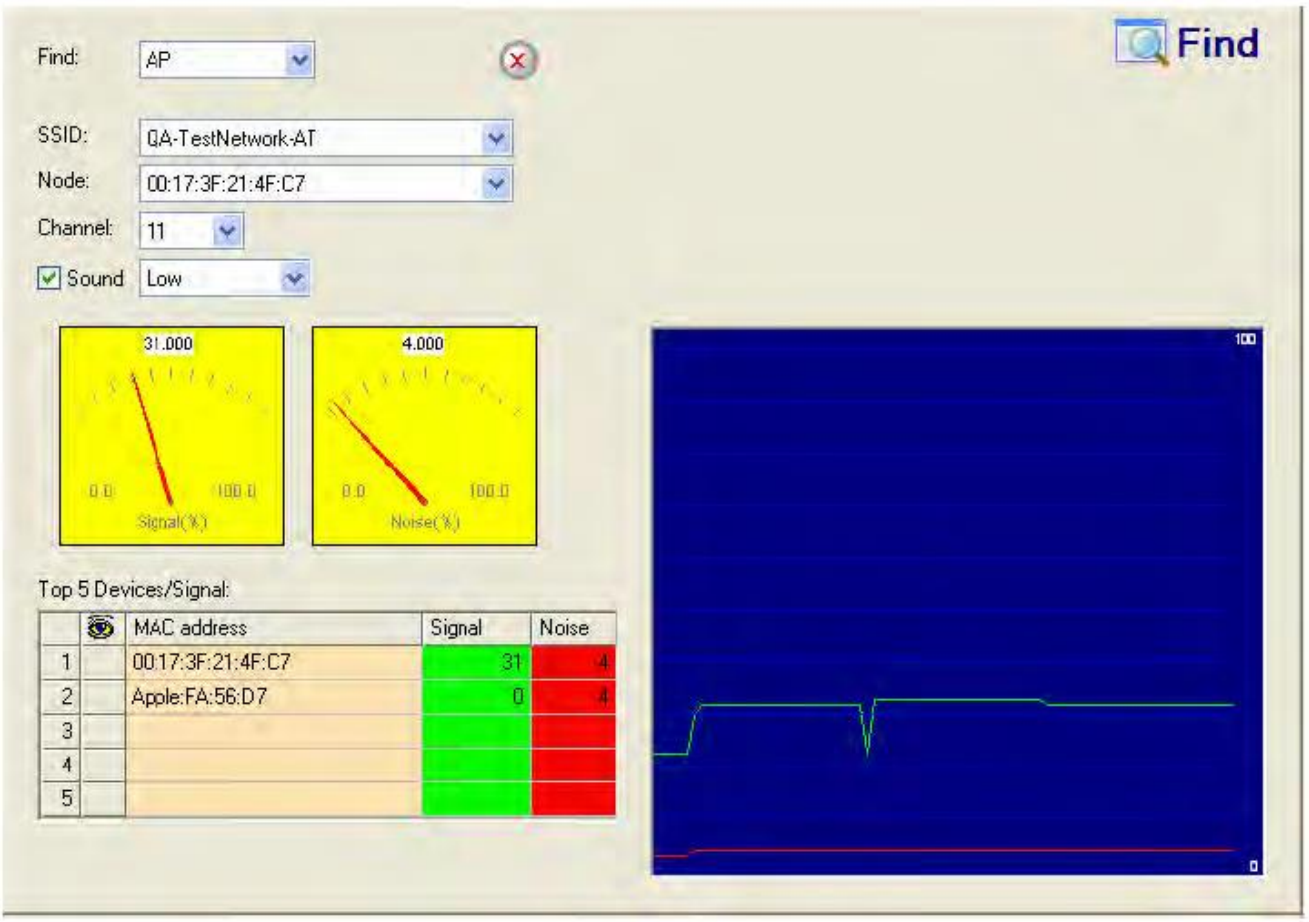
Описание сигнала тревоги и возможные причины

Управление питанием, вероятно, является одной из наиболее важных функций устройств беспроводной локальной сети. Эта функция помогает экономить используемую станциями энергию, удерживая их в состоянии энергосбережения в течение более длительных периодов времени и позволяя получать данные от точки доступа только в определенные интервалы времени.
Беспроводное клиентское устройство должно информировать точку доступа о продолжительности нахождения в спящем режиме (режиме энергосбережения). В конце этого периода времени клиент просыпается и проверяет, ожидают ли его какие-либо кадры данных. После завершения установления связи с точкой доступа клиент может получить кадры данных. Сигналы маяка от точки доступа включают сообщение с индикацией трафика доставки (Delivery Traffic Indication Message - DTIM), информирующее клиента о том, когда ему необходимо проснуться, чтобы принять многоадресный трафик.
Затем точка доступа продолжит буферизацию кадров данных для спящих беспроводных клиентов. Используя карту индикации трафика (Traffic Indication Map - TIM), точка доступа уведомит беспроводного клиента о том, что для него буферизованы данные. Многоадресные кадры передаются после сигнала маяка, включающего DTIM.

Клиент запрашивает доставку буферизованных кадров, передавая на точку доступа кадры PS-Poll. На каждый кадр PS-Poll точка доступа отвечает кадром данных. Если для беспроводного клиента буферизовано много кадров, точка доступа устанавливает в ответе на кадр бит «больше данных». Затем клиент отправляет еще один кадр PS-Poll, чтобы получить следующий кадр данных. Этот процесс продолжается до тех пор, пока клиентом не будут получены все буферизованные кадры данных.
Потенциальный хакер может подделать MAC-адрес беспроводного клиента и отправить поток кадров PS-Poll. В свою очередь, точка доступа отправит буферизованные кадры данных беспроводному клиенту. В действительности, клиент может продолжать находиться в режиме энергосбережения и пропустить эти кадры данных.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer способно обнаружить подобную DoS-атаку, которая может привести к потере легитимных данных беспроводным клиентом. Для поиска исходного устройства и выполнения соответствующих шагов для его удаления из беспроводной среды можно использовать инструмент Find (Найти).



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Rogue AP Traced on Enterprise Wired Network (Неавторизованная точка доступа исследует корпоративную проводную сеть)

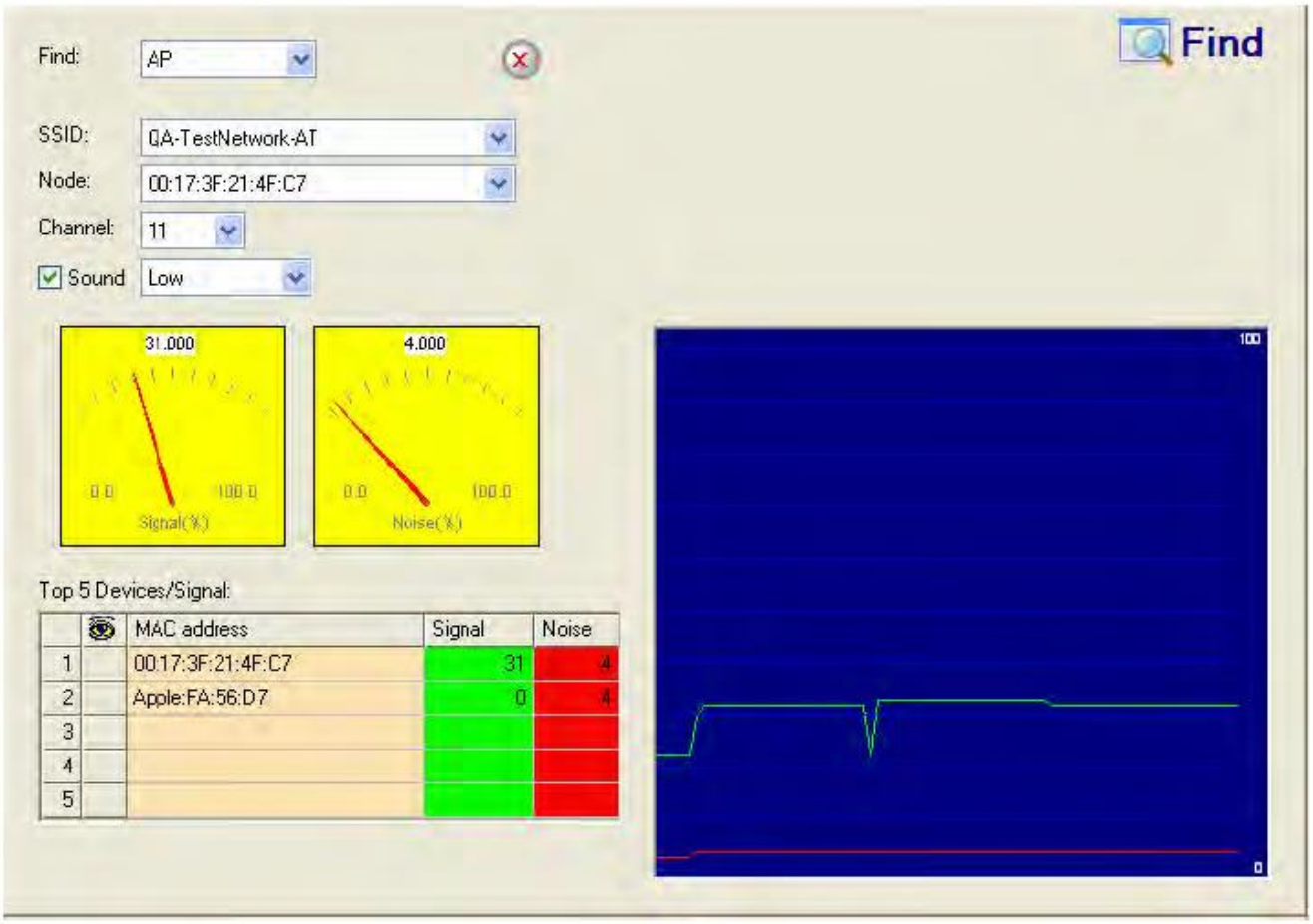
Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer способно обнаруживать неавторизованные точки доступа, подключенные к корпоративной проводной сети. Неавторизованные точки доступа, установленные неавторизованными сотрудниками, могут не соответствовать стандартным корпоративным процедурам развертывания, что поставит под угрозу безопасность беспроводной и проводной сетей. Наличие неавторизованных точек доступа также может указывать на попытки злоумышленников взломать проводную сеть предприятия. Обнаружение приложением AirMagnet WiFi Analyzer неавторизованных устройств должно быть тщательно расследовано. Для использования данной функции убедитесь, что ноутбук с программным обеспечением AirMagnet подключен к проводной сети, отметьте опцию Enable Trace (Включить трассировку) в настройках конфигурации и выберите соответствующий проводной адаптер портативного компьютера, на котором запущено программное обеспечение AirMagnet.

Решение AirMagnet

Как только обнаружена неавторизованная точка доступа, ее можно успешно отследить до корпоративной сети с помощью предусмотренной в приложении AirMagnet WiFi Analyzer функции трассировки проводной сети.

Примечание: Неавторизованная точка доступа, успешно отслеженная приложением AirMagnet WiFi Analyzer до порта корпоративной сети, является «ИСТИННО» мошеннической и на нее необходимо реагировать немедленно. Для физического нахождения местоположения этого мошеннического устройства и выполнения необходимых шагов для его удаления можно использовать инструмент FIND (Найти).

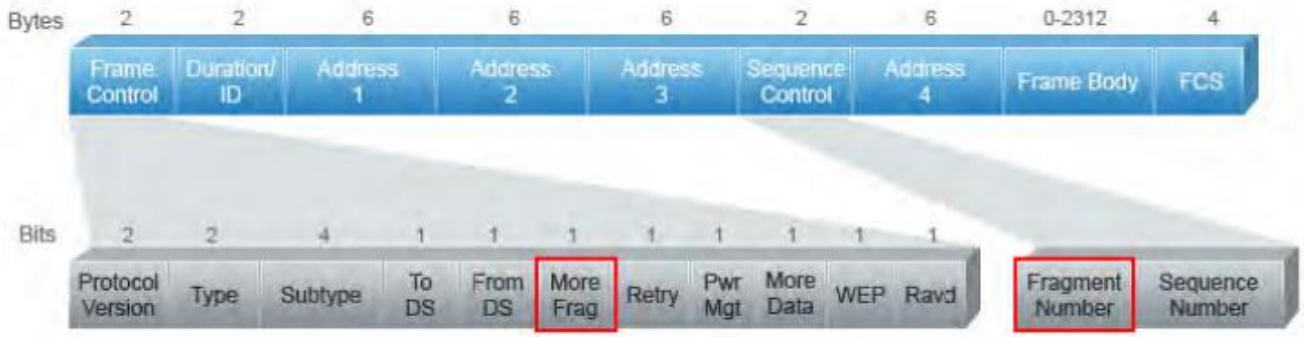


Инструмент Find (Найти) приложения AirMagnet WiFi Analyzer обнаруживает неавторизованную точку доступа, отслеживая уровень ее сигнала

Excessive Fragmentation Degrading Performance (Чрезмерная фрагментация, снижающая производительность)

Описание сигнала тревоги и возможные причины

Уровень MAC стандарта 802.11 поддерживает процессы фрагментации и дефрагментации. Процесс разделения кадра 802.11 на более мелкие кадры для последующей передачи называется фрагментацией; этот процесс помогает повысить надежность и снизить количество ошибок. В случаях, когда характеристики канала ограничивают доступность приема, передача меньшими (фрагментированными) кадрами увеличивает вероятность успеха. Фрагментация выполняется на каждом передатчике непосредственно перед фактическим началом передачи. Процесс рекомбинации фрагментированных кадров в исходный нефрагментированный более длинный кадр называется дефрагментацией. Стандарт IEEE 802.11 определяет формат пакета для идентификации фрагментированных кадров для дефрагментации (показано на рисунке ниже).



Bytes	Байты
Frame Control	Управление кадром
Duration ID	Идентификатор продолжительности
Address	Адрес
Sequence Control	Управление последовательностью
Frame Body	Тело кадра
Bits	Биты
Protocol Version	Версия протокола
Type	Тип
Subtype	Подтип
To DS	К DS
From DS	От DS
More Frag	Больше фрагментов
Retry	Повторная попытка
Pwr Mgt	Управление мощностью
More Data	Больше данных
Rsvd	Зарезервировано
Fragment Number	Номер фрагмента
Sequence Number	Порядковый номер

Поля кадра IEEE 802.11 для фрагментации и дефрагментации кадра

Повышенная надежность фрагментированных кадров меньшего размера достигается за счет служебных данных передачи кадров. Кадр делится на разные сегменты в зависимости от порога фрагментации. Размещение фрагментов в процессе фрагментации определяется «полем управления последовательностью», как показано на рисунке выше. Поле «больше» указывает, является ли фрагмент последним. Если фрагментации и дефрагментации требует слишком много кадров, сетевые служебные данные будут уменьшены, и может возникнуть более серьезная проблема, вызывающая фрагментацию.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает статистику фрагментации в сети и предупреждает о злоупотреблении фрагментацией, которое может привести к снижению производительности сети WLAN. Необходимо тщательно установить порог фрагментации, чтобы сбалансировать получаемые выгоды и

служебные данные. Обычно поставщики оборудования устанавливают порог фрагментации по умолчанию равным 1536. Обратитесь к документации по оборудованию и убедитесь, что рекомендации производителя выполняются.

AP Configuration Changed (SSID) (Изменена конфигурация точки доступа (SSID))

Описание сигнала тревоги и возможные причины

Идентификаторы SSID сети WLAN обычно объявляются в кадрах маяка, отправляемых точками доступа. Они предназначены для того, чтобы клиентские станции могли легко идентифицировать доступные сети WLAN и точки доступа, предоставляющие обслуживание.

Внезапные изменения идентификатора SSID точек доступа могут указывать на то, что неавторизованное лицо получило доступ к этой точке и внесло соответствующие изменения. Любые изменения в идентификаторе SSID могут вызвать прерывание доступа ваших клиентов к сети, поскольку они больше не видят оригинальный идентификатор SSID, настроенный в их утилите клиента или нулевой конфигурации Windows.
Кроме того, злоумышленники, ищущие открытые сети, передвигаясь на автомобиле, и использующие такие инструменты, как Netstumbler, иногда сканируют передаваемые точками доступа идентификаторы SSID для обнаружения потенциальных целей. В случаях, когда ваша сеть транслирует свой идентификатор SSID, она может быть подвержена двум конкретным угрозам:

- Злоумышленники могут установить SSID на своем клиенте, чтобы попытаться подключиться к этой сети WLAN. Согласно большинству веб-сайтов вардрайверов, многие современные точки доступа работают без какой-либо защиты безопасности. Несмотря на то, что знание имени SSID не обязательно означает, что неавторизованные клиенты смогут подключиться к сети, необходимо использовать и другие формы защиты от атак на безопасность (например, DoS-атак).
- Информация о географическом местоположении сети WLAN и точек доступа с координатами GPS может собираться в глобальной базе данных и публиковаться в сети Интернет.

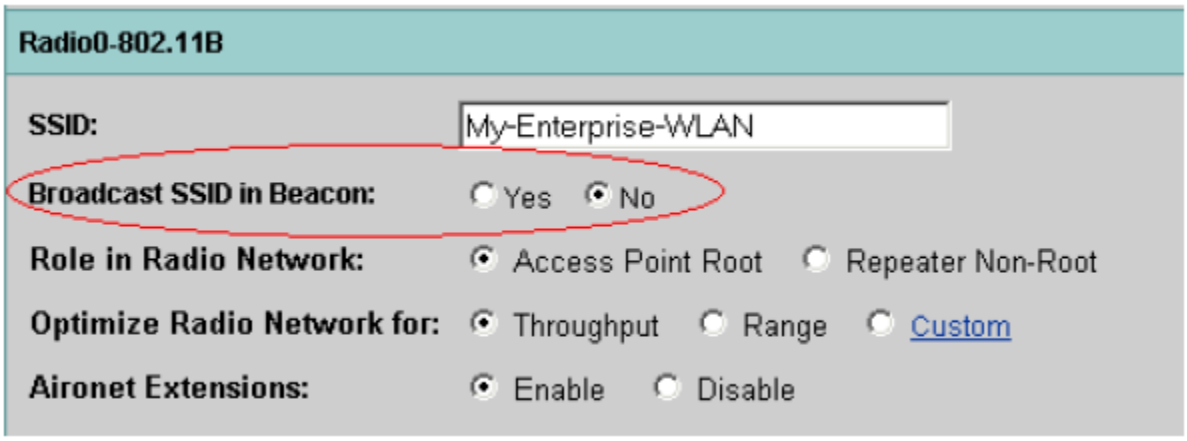
Внезапные изменения в конфигурации «широковещательного SSID» на вашей точке доступа могут указывать на то, что
1. неавторизованное лицо получило доступ к точкам доступа и внесло эти изменения (изменило настройку с Not broadcasting SSID (Не транслировать SSID) на Broadcasting SSID (Транслировать SSID)).
2. администратор точки доступа мог внести изменения для повышения безопасности сети (изменить настройку с Broadcasting SSID (Транслировать SSID) на Not broadcasting SSID (Не транслировать SSID)).

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer также предупреждает пользователя о любых внезапных изменениях идентификатора SSID точки доступа. Это может свидетельствовать о том, что злоумышленник контролирует точку доступа и изменил конфигурацию SSID. Что, в свою очередь, может привести к отключению всех допустимых клиентов от точки доступа, поскольку они теперь не общаются в одной и той же сети, или поставить под угрозу безопасность сети. Подключитесь к точке доступа, конфигурация которой была изменена, и назначьте более надежный пароль входа в точку доступа. Чтобы продолжить предоставление услуг клиентам, измените идентификатор SSID обратно на исходный или восстановите исходное состояние настройки Broadcasting SSID (Транслировать SSID).

Type	CH	Device	MAC	S	N		Security		SSID
AP	7	QA_VoFi_1	00:14:F1:AF:1B:94	58	0	2	?	N	
AP	2	QA_VoFi_3	00:0F:34:A7:78:10	46	0	4	WEP	N	QACiscoVoice
AP	5	QA_VoFi_2	00:12:44:B8:9C:32	26	0	2	WEP	N	QAVOFI
AP	6	192.168.12.1	00:0D:0B:4F:5E:00	79	0	0	Open	N	BuffaloWing_AME
AP	7	QA_VoFi_1	00:14:F1:AF:1B:93	56	0	2	WEP	N	QAVocera
AP	5	QA_VoFi_2	00:12:44:B8:9C:31	27	0	2	802.1x	N	QASpectralink
AP	11	ciscoap1250	00:17:DF:A6:5B:D0	90	0	1	WPA-P	N	EA-Cisco-Jav
AP	7	QA_VoFi_1	00:14:F1:AF:1B:92	55	0	2	WEP	N	QAVOFI
AP	5	QA_VoFi_2	00:12:44:B8:9C:30	25	0	2	WEP	N	QACiscoVoice
AP	7	QA_VoFi_1	00:14:F1:AF:1B:91	57	0	1	802.1x	N	QASpectralink

На экране START приложения AirMagnet WiFi Analyzer нетранслируемый идентификатор SSID отображается красным цветом.



Отключение трансляции SSID для точки доступа Cisco Aironet через интерфейс браузера

Denial-of-Service Attack: Virtual Carrier Attack (Атака типа «отказ в обслуживании»: Атака виртуальной несущей

Описание сигнала тревоги и возможные причины

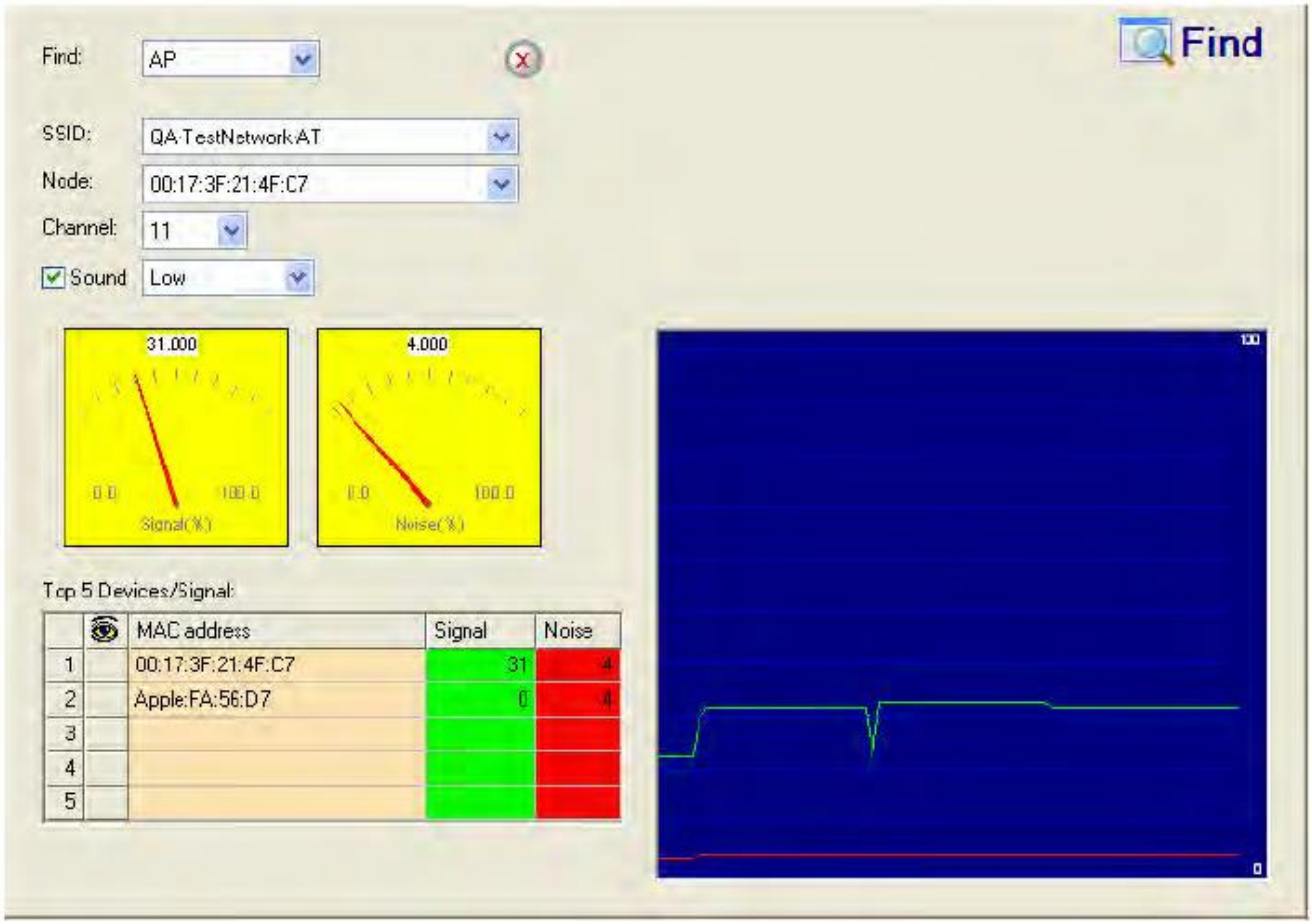
Атака виртуальной несущей осуществляется путем изменения реализации уровня MAC 802.11 для разрешения периодической отправки случайных значений длительности. Эта атака может быть проведена для типов кадров ACK, data, RTS и CTS с использованием больших значений длительности, что позволит злоумышленнику предотвратить доступ к каналу легитимных пользователей.
В обычных условиях кадр ACK должен нести значение большой длительности только тогда, когда ACK является частью фрагментированной последовательности пакетов. Единственный допустимый случай, когда кадр данных может нести значение большой продолжительности, - это подкадр в обмене фрагментированными пакетами.

Один из методов борьбы с этой атакой - установить ограничение на значения продолжительности, принимаемые узлами. Любой пакет, содержащий большее значение продолжительности, просто обрезается до максимально допустимого значения. Можно использовать значения low cap и high cap. Low cap имеет значение, равное количеству времени, необходимому для отправки кадра ACK, плюс отсрочки доступа к среде передачи для этого кадра. Low cap используется, когда единственный пакет, который может следовать за наблюдаемым пакетом - это ACK или CTS. Сюда входят RTS и все кадры управления (подключение и т.п.). С другой стороны, high cap используется, когда допустимо, чтобы пакет данных следовал за наблюдаемым кадром. Предел в этом случае должен включать время, необходимое для отправки самого большого кадра данных, плюс отсрочки доступа к среде передачи для этого кадра. High cap следует использовать в двух местах: при наблюдении за ACK (поскольку ACK может быть частью фрагментированного пакета уровня MAC) и при наблюдении за CTS.

Станция, получившая кадр RTS, также получит кадр данных. Стандарт IEEE 802.11 определяет точное время для последующих кадров CTS и данных. Таким образом, значение продолжительности RTS соблюдается до тех пор, пока не будет получен/не получен следующий кадр данных. Либо наблюдаемый CTS является незапрашиваемым, либо наблюдающий узел является скрытым терминалом. Если этот CTS адресован действительной станции, находящейся в зоне действия, действительная станция может аннулировать его, отправив кадр нулевой функции с нулевой продолжительностью. Если этот CTS адресован станции, находящейся вне зоны действия, одним из методов защиты является введение аутентифицированных кадров CTS, содержащих криптографически подписанную копию предыдущего RTS. Но тогда есть вероятность возникновения проблем со служебными данными и с выполнимостью.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает эту DoS-атаку (атаку типа «отказ в обслуживании»). Найдите устройство и примите соответствующие меры, чтобы удалить его из беспроводной среды.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Fake DHCP Server Detected (Potential Wireless Phishing) (Обнаружен поддельный DHCP-сервер (потенциальный беспроводный фишинг))

Описание сигнала тревоги и возможные причины

Протокол динамической конфигурации хоста (DHCP) используется для назначения динамических IP-адресов устройствам в сети.

Назначение адреса DHCP происходит следующим образом:

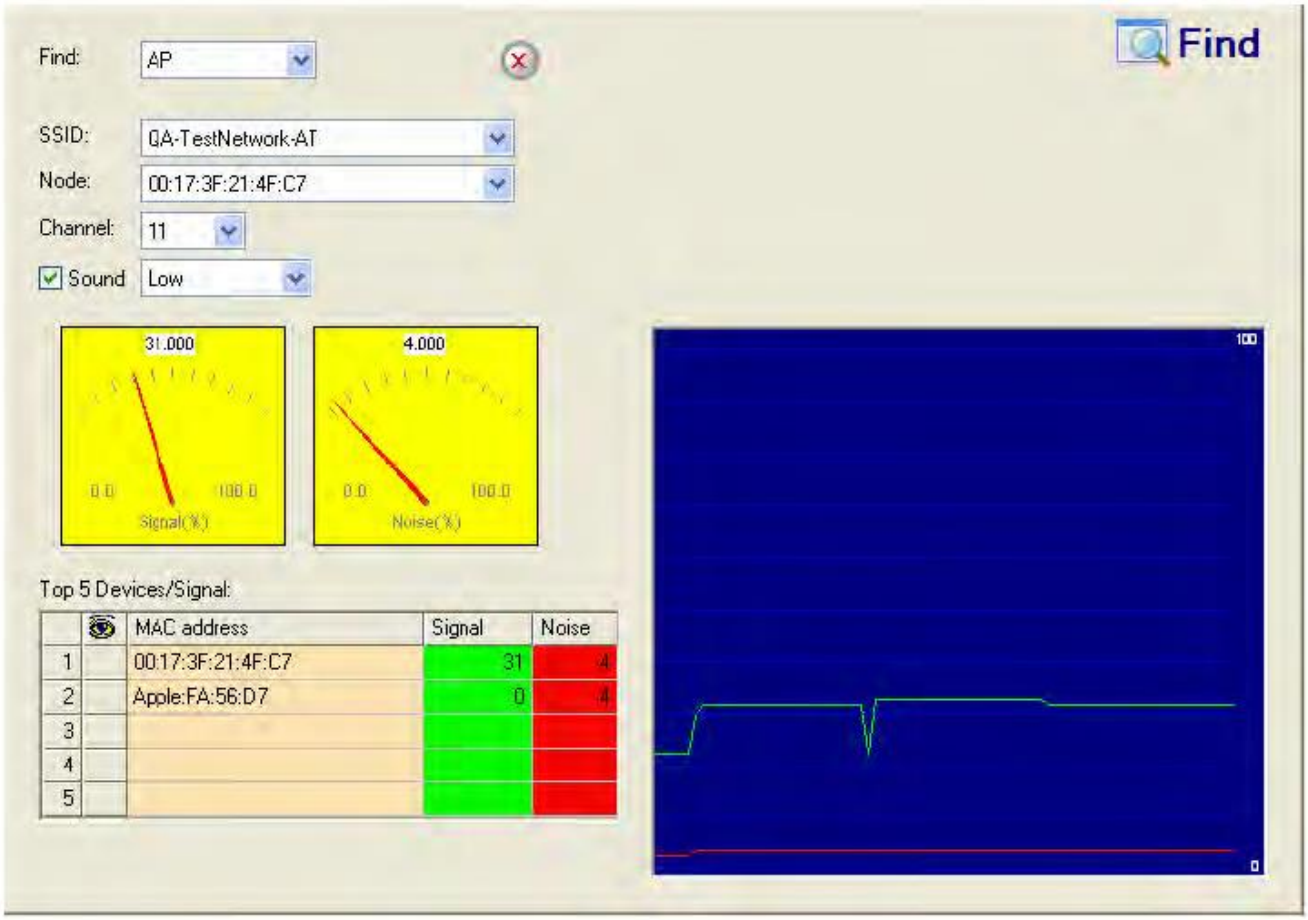
1. Клиентская сетевая карта отправляет пакет обнаружения DHCP, указывая, что ей требуется от DHCP-сервера IP-адрес.
2. Сервер отправляет пакет предложения DHCP с IP-адресом, который он может предложить.

3. Затем клиентская сетевая карта отправляет DHCP-запрос, информируя сервер DHCP о том, что ему нужно назначить предложенный IP-адрес.
4. Сервер возвращает DHCP ACK, подтверждая, что сетевая карта отправила запрос на определенный IP-адрес. На этом этапе интерфейс клиента назначает/связывает первоначально предложенный DHCP-сервером IP-адрес.

DHCP-сервер должен быть выделенным компьютером, который является частью проводной сети предприятия или может быть беспроводным/проводным шлюзом. Однако служба DHCP может ненамеренно или злонамеренно работать на других беспроводных устройствах для нарушения работы IP-службы WLAN. Поскольку у беспроводных клиентов, запрашивающих IP-адрес у DHCP-сервера, нет никаких средств для какой-либо аутентификации сервера, они могут непреднамеренно подключиться к таким поддельным DHCP-серверам для получения своих IP-адресов. Поддельные DHCP-серверы могут предоставлять клиентам нефункциональные сетевые конфигурации или перенаправлять через них весь клиентский трафик. Это даст хакерам возможность подслушивать каждый пакет, отправленный клиентом. С помощью поддельных DNS-серверов хакер может также отправлять пользователей на поддельные веб-страницы, требующие от них входа в систему, что даст злоумышленнику учетные данные (имя пользователя и пароль). Также он может просто выдавать нефункциональные и немаршрутизируемые IP-адреса для выполнения DoS-атаки. Этот вид атак обычно направлен на сети WLAN без шифрования, например, на публичные точки доступа или сети торговых выставок.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает беспроводные станции, на которых запущена служба DHCP, предоставляющая IP-адреса ничего не подозревающим пользователям. После того, как клиент идентифицирован, и приложение AirMagnet WiFi Analyzer о нем сообщило, администратор сети WLAN может использовать инструмент FIND (Найти) для определения местоположения устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Device Unprotected by Other Encryption (Устройство не защищено другим шифрованием)

Описание сигнала тревоги и возможные причины

Если развернутая система безопасности сети WLAN требует использования технологий шифрования, предоставляемых Cranite Systems, Inc., можно включить этот сигнал тревоги приложения AirMagnet WiFi Analyzer, который будет предупреждать вас об устройствах, которые участвуют в обмене данными в сети WLAN без шифрования Cranite.

Программное обеспечение Cranite WirelessWall обеспечивает надежную безопасность беспроводной сети, беспрепятственную мобильность и улучшенную видимость сети, при этом соблюдая строгий государственный стандарт безопасности FIPS 140-2. Оно шифрует полные кадры Ethernet, а не только полезные данные IP, скрывая от неавторизованных приемников такую важную информацию, как IP-адреса, приложения и порты.

Шифрование на уровне кадров также защищает от взлома и использования для атаки на сеть сетевой трафик, не связанный с данными, включая запросы DHCP или сообщения ARP. В отличие от решений на основе IPSec, шифрование на уровне кадров позволяет легко использовать другие протоколы, например, IPX и AppleTalk.

Приложение AirMagnet WiFi Analyzer позволяет администраторам корпоративной сети контролировать, администрировать и защищать сети WLAN своей организации в любом количестве кампусов и офисов, а также погружаться в отдельные элементы сети с помощью интерфейса удаленного управления. Приложение AirMagnet WiFi Analyzer выявляет более 100 различных типов беспроводных проблем, обеспечивая комплексную систему управления безопасностью, надежностью и производительностью, которая контролирует каждый диапазон и канал сети WLAN, используемые во всем мире (802.11a, 802.11b или 802.11g), независимо от того, насколько они велики или рассредоточены.

Решение AirMagnet

Примите соответствующие меры, чтобы включить использование шифрования Cranite для различных устройств в беспроводной среде. Данное новое предупреждение системы безопасности идентифицирует пользователей, которые не могут использовать технологию Cranite WirelessWall. Это позволит заботящимся о безопасности клиентам, которые выбрали WirelessWall, быть уверенными, что их политики аутентификации/шифрования соблюдаются при каждой установке по всему миру. Кроме того, общие уведомления для обеих систем позволят администраторам Cranite видеть внешние угрозы для беспроводной сети. Интеграция тревог AirMagnet в WirelessWall позволит пользователям Cranite лучше видеть общую производительность своей сети и выявлять такие внешние угрозы, как DoS-атаки. Комбинированное предложение продуктов включает сертифицированное государством программное обеспечение Cranite WirelessWall, которое обеспечивает безопасность беспроводных локальных сетей (LAN), и систему управления безопасностью и производительностью AirMagnet WiFi Analyzer, которая контролирует и управляет безопасностью беспроводной сети. С помощью этого решения организации получают преимущества от сертифицированной государством безопасности уровня 2, свободного роуминга и взаимной аутентификации в сочетании с наиболее полным мониторингом мошенников, беспроводных атак и сетевых вторжений.

Denial-of-Service Attack: Queensland University of Technology Exploit (Атака типа «отказ в обслуживании»: использование разработки Технологического университета Квинсленда)

Уязвимость, связанная с отказом в обслуживании в беспроводных устройствах IEEE 802.11: US-CERT VU # 106678 и Aus-CERT AA-2004.02

Описание сигнала тревоги и возможные причины

Устройства WLAN 802.11 в качестве основного механизма доступа используют множественный доступ с контролем несущей и предотвращением конфликтов (CSMA/CA), при котором устройство WLAN перед началом любой передачи прослушивает среду и отключает передачу, когда обнаруживает любую уже осуществляющуюся передачу. Предотвращение коллизий сочетает в себе механизм физического распознавания, а также механизм виртуального распознавания, который включает в себя вектор распределения сети (NAV), время, до которого среда становится доступной для передачи. Оценка состояния канала (CCA) в протоколе DSSS определяет, свободен ли канал WLAN для того, чтобы устройство 802.11b могло осуществлять по нему передачу.

Марк Луи, Кристиан Вуллемс, Кевин Там и Джейсон Смит из Центра исследования информационной безопасности Технологического университета Квинсленда в Брисбене, Австралия, недавно обнаружили недостаток в стандарте протокола 802.11b, который потенциально может сделать его уязвимым для DoS-атаки RF Jamming (Преднамеренные радиочастотные помехи).

Эта атака специально направлена на нарушение работы функции CCA (Оценка состояния канала). Согласно бюллетеню AusCERT, «атака на эту уязвимость использует функцию CCA на физическом уровне и заставляет все узлы WLAN в пределах досягаемости не только клиентов, но и точки доступа, откладывать передачу данных на время атаки. При атаке устройство ведет себя так, как будто канал всегда занят, что предотвращает передачу любых данных по беспроводной сети».

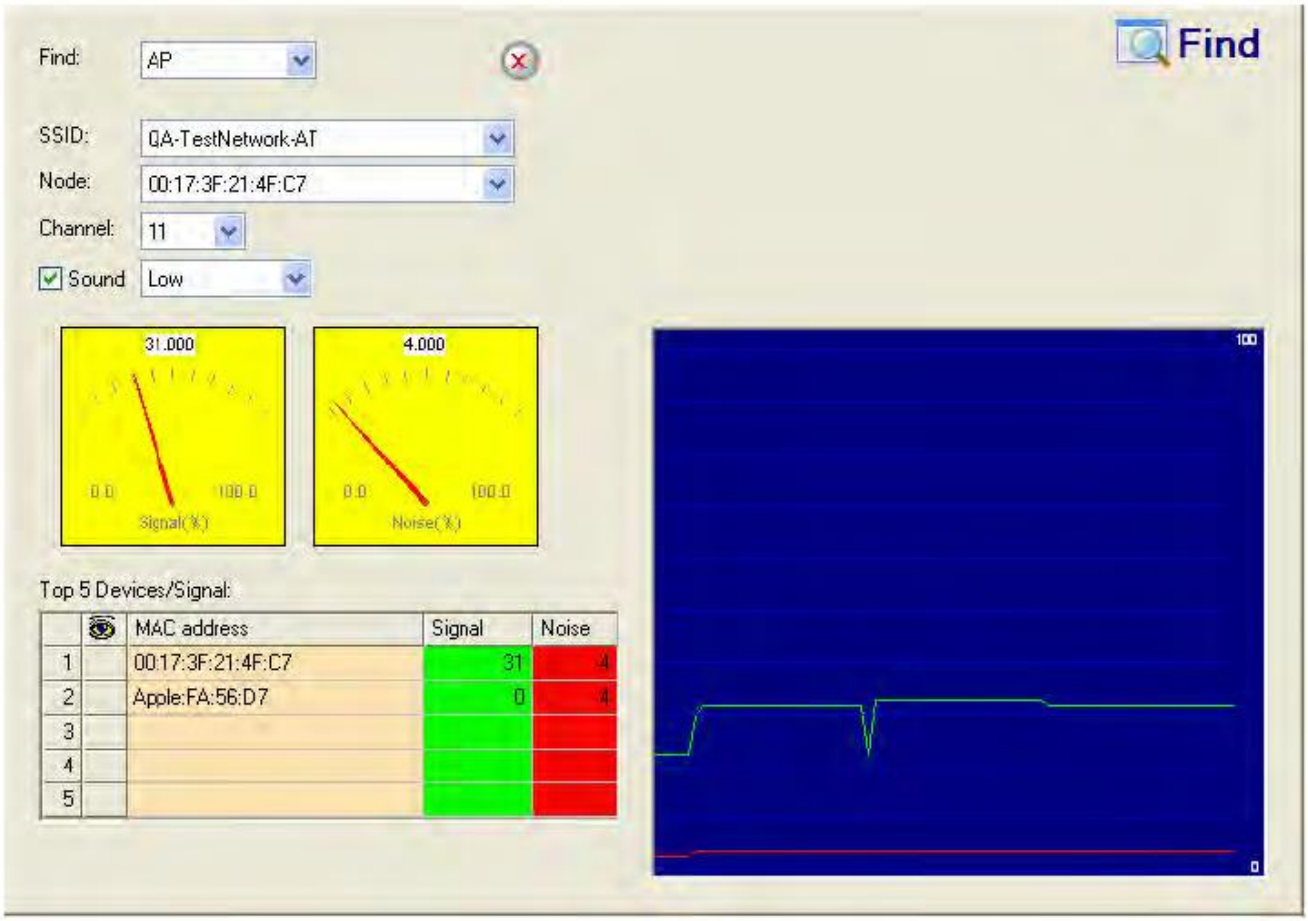
Эта DoS-атака затрагивает устройства WLAN DSSS, включая IEEE 802.11, 802.11b и низкоскоростные (ниже 20 Мбит/с) беспроводные устройства 802.11g. Беспроводные устройства IEEE 802.11a (с использованием OFDM), высокоскоростные (выше 20 Мбит/с с использованием OFDM) стандарта 802.11g не подвержены данной атаке. Также она не влияет на устройства, использующие FHSS.

Любой злоумышленник, использующий КПК или портативный компьютер с картой WLAN, может запустить такую атаку на SOHO и корпоративные сети WLAN. Единственным решением или известной защитой от такой атаки является переход на протокол 802.11a.

Для получения дополнительной информации об этой DoS-атаке, пожалуйста, обратитесь к:
www.isi.qut.edu.au/
http://www.auscert.org.au/render.html?it=4091
http://www.kb.cert.org/vuls/id/106678

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает эту конкретную DoS-атаку и подает сигнал тревоги. Используйте инструмент Find (Найти), чтобы найти ответственное устройство и предпринять соответствующие шаги для его удаления из беспроводной среды.



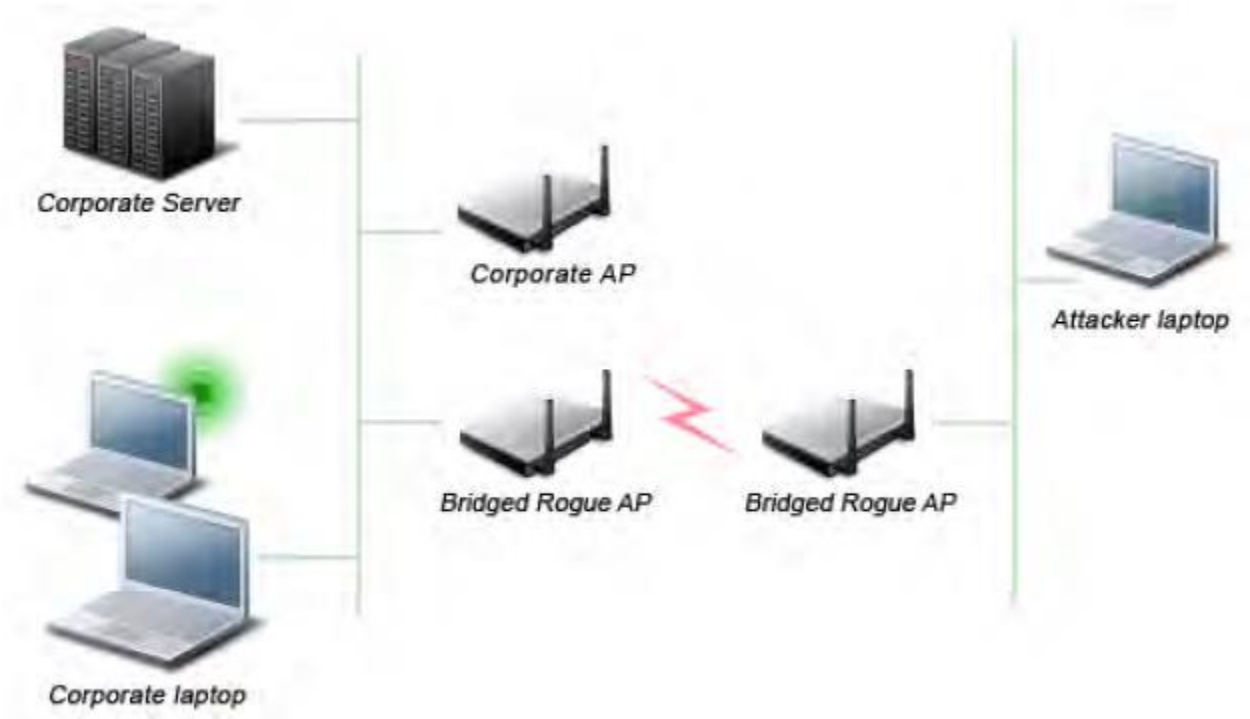
Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

AP Operating in Bridged Mode Detected (Обнаружена точка доступа, работающая в мостовом режиме)

Описание сигнала тревоги и возможные причины

Точки доступа являются наиболее часто используемыми инфраструктурными устройствами сетей WLAN. Точка доступа действует как централизованный концентратор, через который различные беспроводные устройства могут подключаться к проводной распределительной сети. Существуют точки доступа, которые могут работать как в режиме точки доступа, так и в мостовом режиме. Большинство из них могут работать одновременно только в одном из этих режимов, хотя есть устройства нескольких производителей, которые поддерживают оба режима одновременно. В мостовом режиме беспроводный мост можно использовать для соединения друг с другом двух проводных сегментов локальной сети. Это может быть конфигурация точка-точка или точка-многоточка.

Злоумышленник или мошенник может установить внутри корпоративной сети такой беспроводной мост, который неминуемо расширит ее до любого места за пределами корпоративной территории. Обнаружение подобных беспроводных мостовых устройств указывает на то, что что-то не так и безопасность корпоративной сети может быть скомпрометирована.

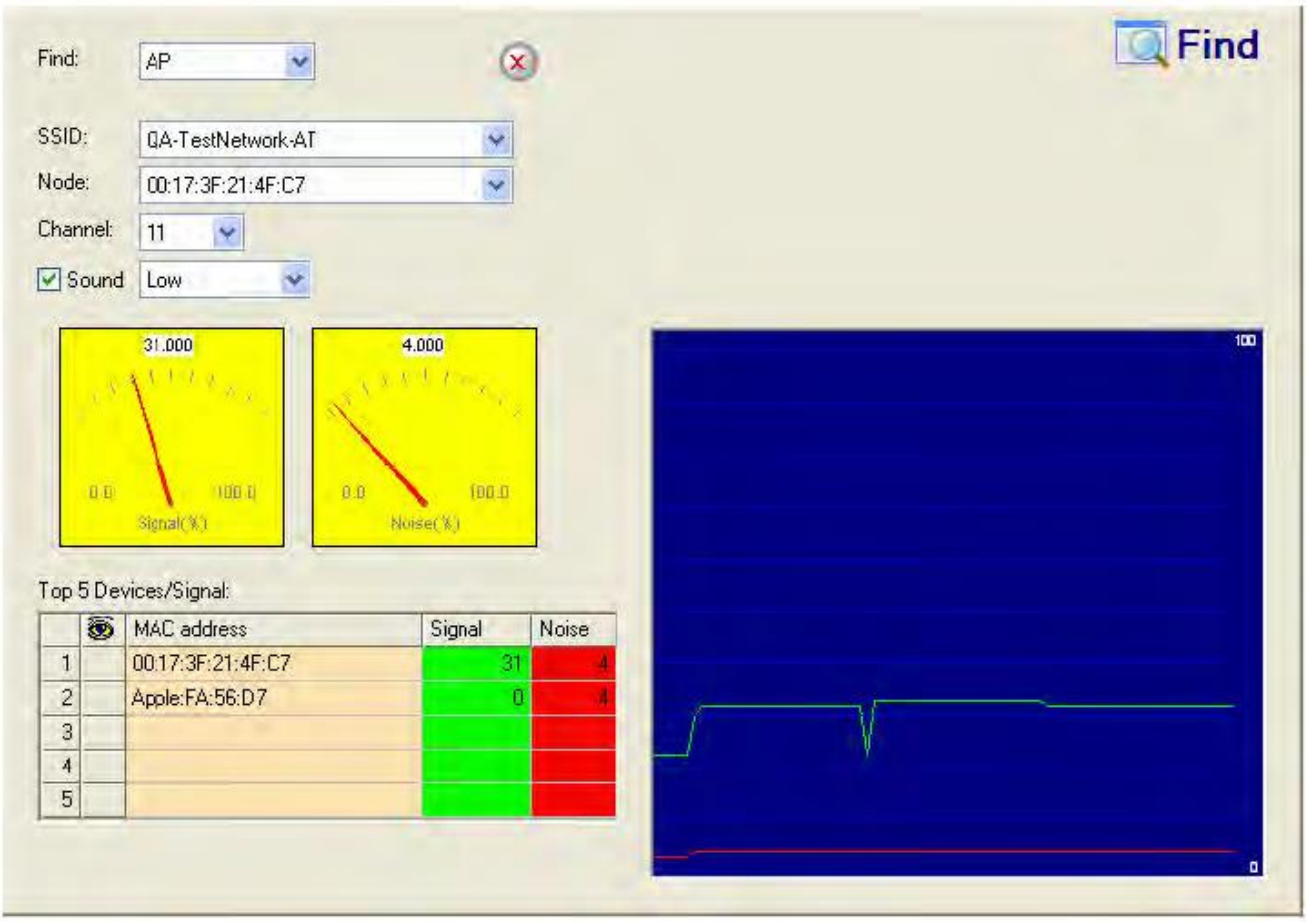


Corporate Server	Корпоративный сервер
Corporate AP	Корпоративная точка доступа
Attacker Laptop	Ноутбук злоумышленника
Bridged Rogue AP	Неавторизованная мостовая точка доступа
Corporate Laptop	Корпоративный ноутбук

Злоумышленник подключает неавторизованную мостовую точку доступа/беспроводной мост к корпоративной сети и ставит ее безопасность под угрозу

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer предупредит администратора об обнаружении беспроводного моста. Как только работающая в мостовом режиме неавторизованная точка доступа будет идентифицирована и о ней сообщит приложение AirMagnet WiFi Analyzer, администратор WLAN сможет использовать инструмент FIND (Найти), чтобы определить местонахождение неавторизованного устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

EAP Attack Against 802.1x Authentication Type (Атака EAP на тип аутентификации 802.1x)

Описание сигнала тревоги и возможные причины

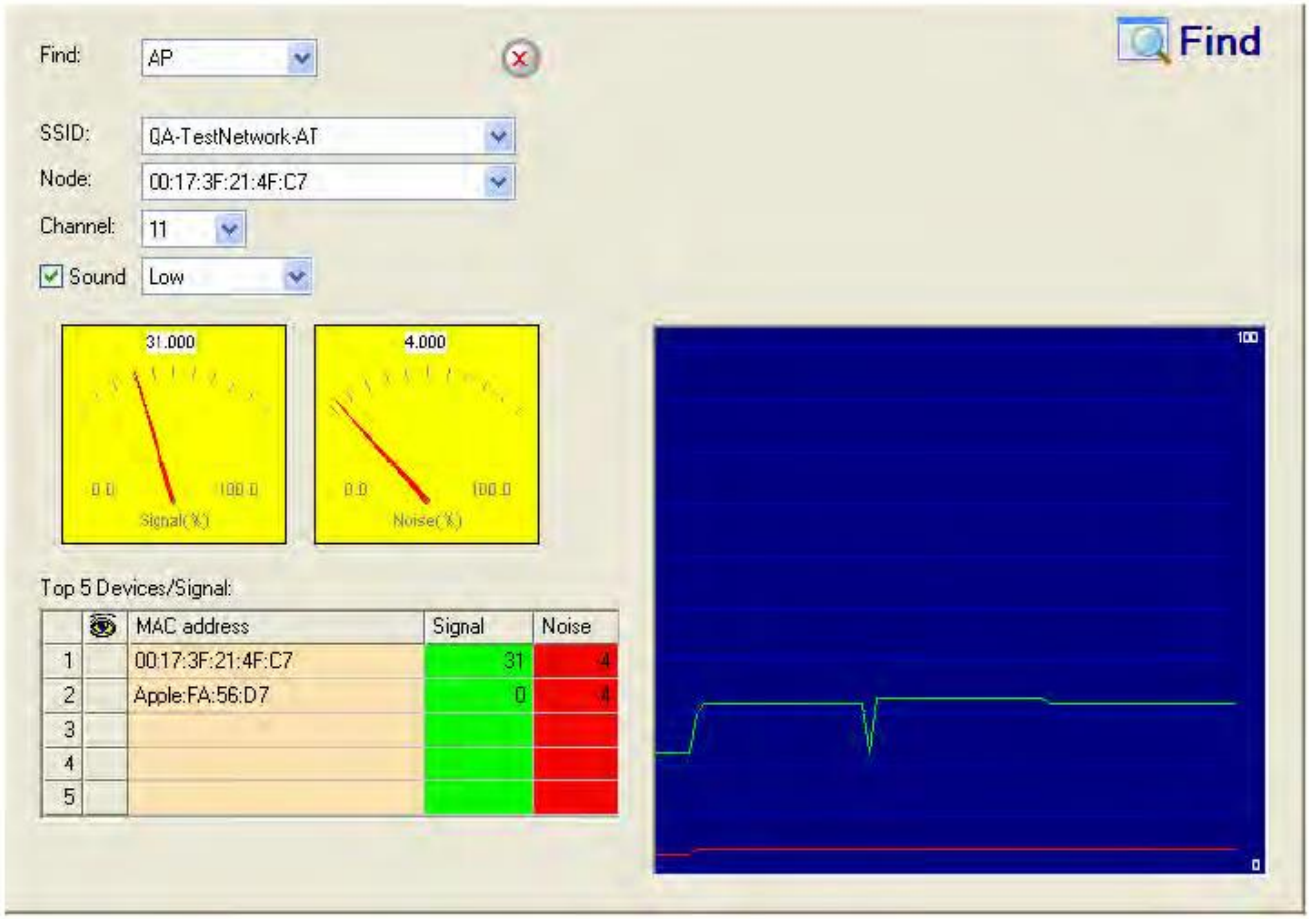
IEEE 802.1x предоставляет структуру EAP (Extensible Authentication Protocol – протокол расширенной аутентификации) для проводной или беспроводной аутентификации в сетях LAN. Структура EAP позволяет гибко реализовать протокол аутентификации. Поставщики беспроводного оборудования, поддерживающего 802.1x или WPA, реализуют такие протоколы аутентификации, как LEAP, MD5, OTP (одноразовый пароль), TLS, TTLS, EAP-FAST и т.д. Некоторые из этих протоколов аутентификации основаны на использовании имени пользователя и пароля, при котором имя пользователя передается в открытом виде без шифрования, а пароль используется для ответа на вопросы аутентификации.

Большинство алгоритмов аутентификации на основе паролей подвержены атакам по словарю. Во время атаки по словарю злоумышленник получает имя пользователя в результате обмена данными по протоколу незашифрованной идентификации 802.1x. Затем злоумышленник пытается угадать пароль пользователя и получить доступ к сети, используя каждое «слово» в словаре наиболее часто используемых паролей или возможные комбинации паролей. Атака по словарю основана на том факте, что паролем часто является обычное слово, имя или сочетание слов или имен с незначительными модификациями, например, одной или двумя цифрами в конце.

Злоумышленники с легитимной комбинацией идентификатора пользователя 802.1x и пароля (или действующим сертификатом) смогут проникнуть в процесс аутентификации 802.1x без надлежащего знания точного типа EAP. Злоумышленник будет пробовать различные типы EAP, например, TLS, TTLS, LEAP, EAP-FAST, PEAP и т.д. до успешного входа в сеть. Это делается методом проб и ошибок, так как существует лишь несколько типов EAP, которые злоумышленник может попробовать использовать, чтобы каким-либо образом пройти аутентификацию в сети.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает подобную попытку злоумышленника получить доступ к сети с использованием различных типов аутентификации 802.1x. Примите соответствующие меры, чтобы найти устройство и удалить его из беспроводной среды. Для этого воспользуйтесь инструментом FIND (Найти).



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Potential Honey Pot AP Detected (Обнаружена потенциальная точка доступа Honey Pot)

Описание сигнала тревоги и возможные причины

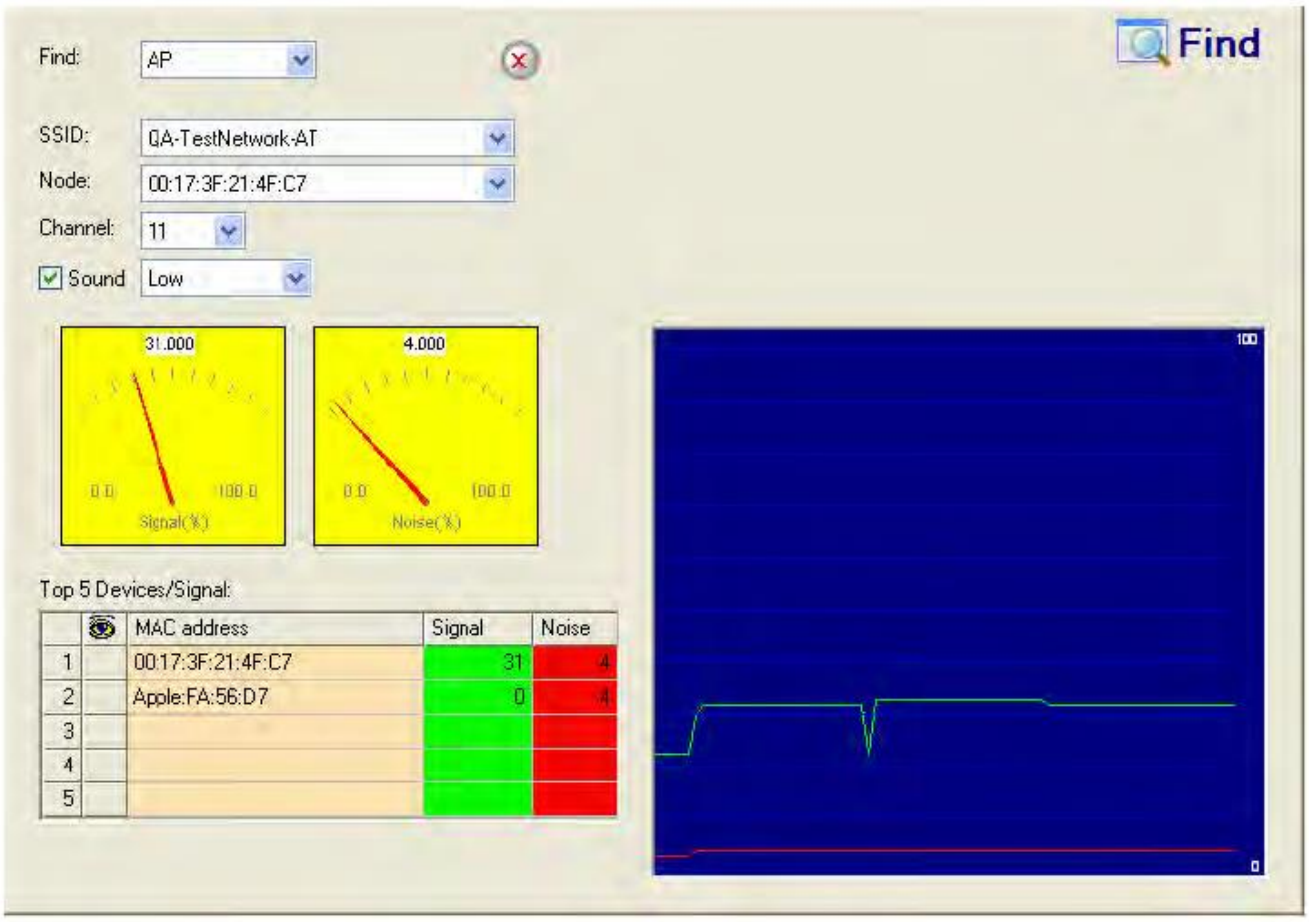
Добавление беспроводной сети WLAN в корпоративную среду формирует новый класс угроз сетевой безопасности. Радиочастотные сигналы, которые проникают через стены и выходят за намеченные границы, могут сделать сеть доступной для неавторизованных пользователей. Мошенническая точка доступа может подвергнуть всю корпоративную сеть риску проникновения и атаки извне. Не преуменьшая угрозу, исходящую от мошеннической точки доступа, следует сказать, что существует множество других угроз безопасности беспроводной сети и вторжений, таких как неправильно настроенная точка доступа, ненастроенная точка доступа и DoS-атаки (атаки типа «отказ в обслуживании»).

Одна из наиболее эффективных атак, с которыми сталкиваются корпоративные сети, использующие беспроводную связь, это использование точки доступа Honey pot. Злоумышленник может использовать различные инструменты, например, NetStumbler, Wellenreiter, MiniStumbler и так далее, чтобы узнать SSID корпоративной точки доступа. Затем злоумышленник может установить точку доступа за пределами здания или, если возможно, внутри помещения, и транслировать ранее обнаруженный корпоративный SSID. Любой ничего не подозревающий клиент может подключиться к этой точке доступа Honey pot с более высоким уровнем сигнала. После подключения злоумышленник получит возможность предпринять

различные атаки на клиентскую станцию, поскольку теперь трафик будет перенаправляться через подставную точку доступа.

Решение AirMagnet

После того, как точка доступа Honeypot идентифицирована и о ней получена информация от приложения AirMagnet WiFi Analyzer, администратор сети WLAN может использовать инструмент FIND (Найти) для определения местоположения мошеннического устройства.

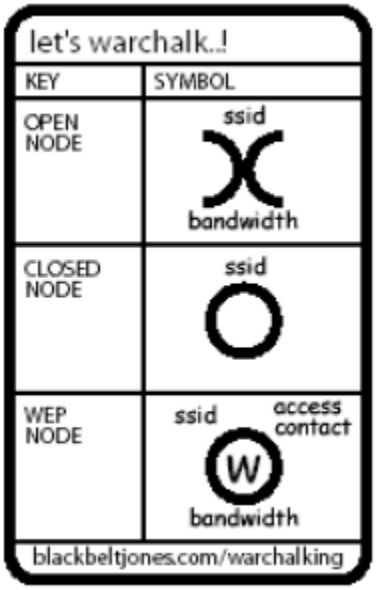


Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

NetStumbler Detected (Обнаружено устройство с NetStumbler)

Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer обнаруживает беспроводную клиентскую станцию, зондирующую сеть WLAN на предмет анонимного подключения (то есть запросы связи с точкой доступа с любым идентификатором SSID) с помощью инструмента NetStumbler. Сигнал тревоги Device probing for AP (Устройство, зондирующее точку доступа) подается, когда хакеры используют новейшие версии инструмента NetStumbler. Для более старых версий приложение AirMagnet Enterprise подает сигнал тревоги NetStumbler detected (Обнаружен NetStumbler).



Злоумышленник обнародует обнаруженную сеть WLAN и ее конфигурацию в месте развертывания сети WLAN с помощью этих универсальных символов.

NetStumbler - это наиболее широко используемый инструмент для обнаружения доступных беспроводных сетей при перемещении на автомобиле или пешком. Хакер при перемещении на автомобиле использует специальные инструменты для обнаружения точек доступа и публикации информации о них (MAC-адрес, идентификатор SSID, реализованная безопасность и т.д.) в сети Интернет с указанием географического местоположения точек доступа. Злоумышленники, передвигающиеся пешком, обнаруживают точки доступа WLAN и отмечают конфигурацию WLAN в общественных местах универсальными символами, показанными выше. Оба эти метода не отличаются в принципе, за исключением способа передвижения – пешком или на автомобиле. Веб-сайт NetStumbler (http://www.netstumbler.com/) предлагает программное обеспечение MiniStumbler для использования на карманных компьютерах, что избавляет злоумышленника от необходимости носить тяжелый ноутбук. Также он поддерживает больше карт по сравнению с Wellenreiter, еще одним широко используемым инструментом сканирования. Пешие злоумышленники любят использовать MiniStumbler и аналогичные продукты для обследования торговых центров и крупных розничных магазинов. Кроме того, поиск беспроводных сетей осуществляется и с воздуха. Используется то же оборудование, но из низколетящего частного самолета с мощными антеннами. Сообщалось, что такой хакер из города Перт в Австралии во время полета получал сообщения электронной почты и сеансы Internet Relay Chat (ретранслируемого интернет-чата) с высоты 1500 футов (450 метров).

Расположение точек доступа 802.11, опубликованное в Интернете группами war-driving (передвигающимися на автомобилях)

Решение AirMagnet

Чтобы предотвратить обнаружение ваших точек доступа этими средствами взлома, можно настроить точки доступа так, чтобы они не транслировали свой идентификатор SSID. Чтобы увидеть, какие из ваших точек доступа транслируют (объявляют) свои идентификаторы SSID в сигналах маяка, используйте приложение AirMagnet WiFi Analyzer.

AP Using Default Configuration (Точка доступа, использующая конфигурацию по умолчанию)

Описание сигнала тревоги и возможные причины

Поставляемые производителями беспроводного оборудования точки доступа обычно имеют набор параметров конфигурации, настроенных по умолчанию. Пока эти параметры конфигурации не будут настроены в соответствии с вашей корпоративной политикой безопасности, новые точки доступа не следует подключать к корпоративной проводной сети. Ненастроенные точки доступа имеют пароль администратора, идентификаторы SSID, каналы, параметры аутентификации/шифрования, строки комьюнити для чтения/записи SNMP и другие параметры, настроенные по умолчанию в зависимости от производителя. Такие значения по умолчанию являются общедоступными, они указаны в руководствах пользователя и руководствах по установке на веб-сайте производителя, и могут использоваться хакерами для обхода системы безопасности WLAN.

SSID по умолчанию	Производитель/продукты
tsunami	Cisco Aironet
Compaq	Compaq WL-100/200/300/400
WLAN	D-Link DL-713
WLAN	SMC SMC2652W/SMC2526W
comcomcom	3Com AirConnect
Intel	Intel Pro/Wireless 2011
AirPort Network	Apple Airport
Mello	ZCOMMax XWL 450
Имя сети по умолчанию для Roamabout	Точки доступа Lucent, Cabletron или Enterasys
Bridge	SMC SMC2682
MAC-адрес	SOHOware NetBlaster

Примеры SSID по умолчанию для точек доступа от разных поставщиков беспроводного оборудования

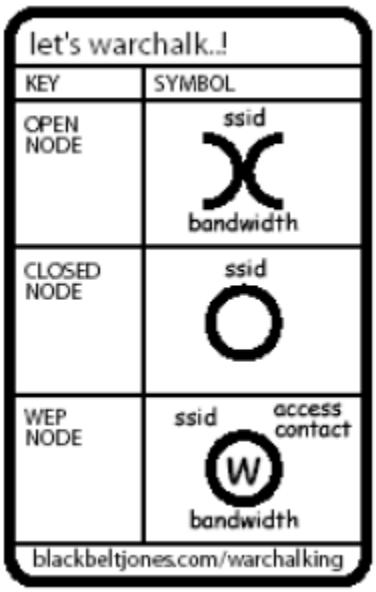
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer сканирует сеть WLAN в поиске ненастроенных точек доступа, сопоставляя заводские настройки по умолчанию с внутренней базой данных хорошо известных конфигураций по умолчанию, например, SSID. При обнаружении совпадения приложение AirMagnet WiFi Analyzer предупреждает администратора WLAN о ненастроенной точке доступа. Чтобы избежать легкого взлома точки доступа, администратор должен изменить ее настройки по умолчанию.

Wellenreiter Detected (Обнаружено устройство с Wellenreiter)

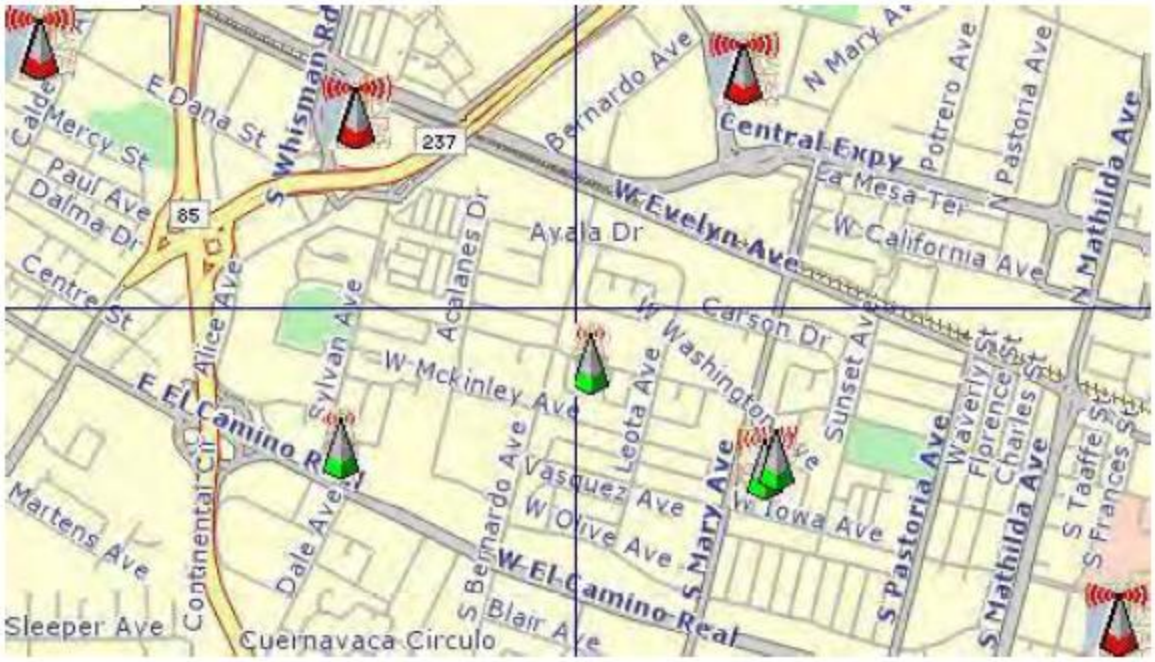
Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer обнаруживает беспроводную клиентскую станцию, зондирующую сеть WLAN на возможность анонимного подключения (то есть запросы связи с точкой доступа с любым идентификатором SSID) с помощью инструмента Wellenreiter.



Злоумышленник (War-chalker) обнародует обнаруженную сеть WLAN и ее конфигурацию в месте развертывания сети WLAN с помощью этих универсальных символов.

Wellenreiter - это широко используемый инструмент для обнаружения доступных беспроводных сетей при перемещении на автомобиле или пешком. Хакер при перемещении на автомобиле использует этот инструмент для обнаружения точек доступа и публикации информации о них (MAC-адрес, SSID, реализованная безопасность и т.д.) в сети Интернет с указанием географического местоположения точек доступа. Злоумышленники, передвигающиеся пешком, обнаруживают точки доступа WLAN и отмечают конфигурацию WLAN в общественных местах универсальными символами, показанными выше. Оба эти метода не отличаются в принципе, за исключением способа передвижения – пешком или на автомобиле. Пешие злоумышленники любят использовать Wellenreiter и аналогичные продукты для обследования торговых центров и крупных розничных магазинов. Кроме того, поиск беспроводных сетей осуществляется и с воздуха. Используется то же оборудование, но из низколетящего частного самолета с мощными антеннами. Сообщалось, что такой хакер из города Перт в Австралии во время полета получал сообщения электронной почты и сеансы Internet Relay Chat (ретранслируемого интернет-чата) с высоты 1500 футов (450 метров).



Расположение точек доступа 802.11, опубликованное в Интернете группами war-driving (передвигающимися на автомобилях)

Инструмент поддерживает карты на базе Prism2, Lucent и Cisco. Он позволяет обнаруживать инфраструктуру и сети ad-hoc, если эти сети транслируют свои идентификаторы SSID, свои возможности WEP и автоматически предоставляют информацию о производителе. Также инструмент создает файл дампа, совместимый с ethereal/tcpdump, и файл сохранения приложения. Также имеется поддержка GPS. Пользователи могут загрузить инструмент с http://sourceforge.net/projects/wellenreiter/

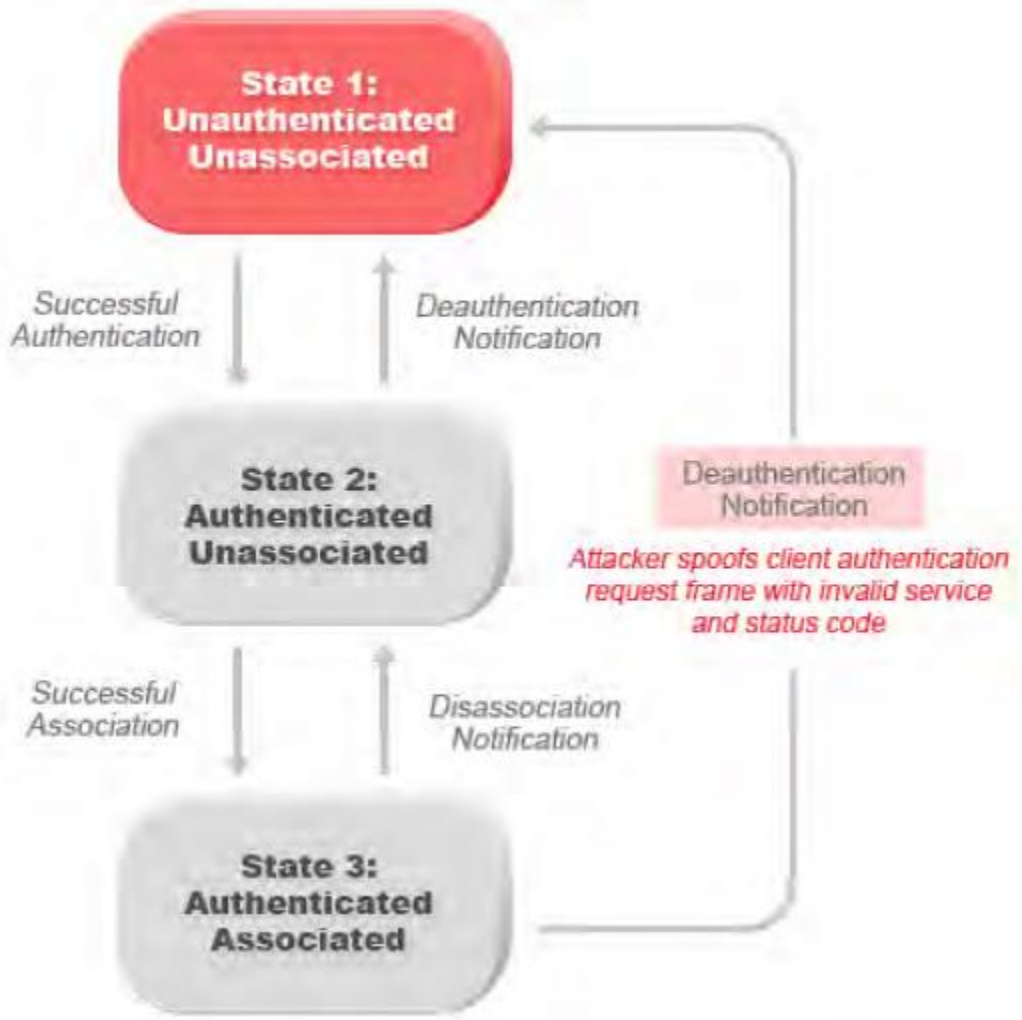
Решение AirMagnet

Чтобы предотвратить обнаружение ваших точек доступа этими средствами взлома, можно настроить эти точки так, чтобы они не транслировали свой идентификатор SSID. Чтобы увидеть, какие из ваших точек доступа транслируют (объявляют) свои идентификаторы SSID в сигналах маяка, используйте приложение AirMagnet WiFi Analyzer.

Denial-of-Service Attack: FATA-Jack Tool Detected (Атака типа «отказ в обслуживании»: Обнаружен инструмент FATA-Jack)

Описание сигнала тревоги и возможные причины

Для отслеживания аутентификации станции и проверки статуса ее подключения IEEE 802.11 задает машину состояний клиента. Беспроводные клиенты и точки доступа реализуют такую машину состояний (смотрите рисунок ниже) на основе стандарта IEEE. Успешно подключенная клиентская станция для продолжения беспроводной связи должна оставаться в Состоянии 3. Клиентская станция в Состоянии 1 или Состоянии 2 не может участвовать в процессе передачи данных по сети WLAN до тех пор, пока для достижения Состояния 3 она не будет аутентифицирована и подключена. Стандарт IEEE 802.11 также задает две службы аутентификации: Open System Authentication (Открытая системная аутентификация) и Shared Key Authentication (Аутентификация с совместно используемым ключом). Для установления связи с точкой доступа беспроводные клиенты проходят один из двух процессов аутентификации.



State 1: …	Состояние 1: Аутентификация не пройдена, нет соединения
Successful Authentication	Успешная аутентификация
Deauthentication Notification	Извещение о деаутентификации
State 2:…	Состояние 2: Аутентификация пройдена, нет соединения
Attacker spoofs client authentication request…	Злоумышленник фабрикует кадр запроса аутентификации клиента с неверным кодом службы и состояния
Successful Association	Успешное подключение
Diassociation Notification	Извещение о разъединении
State 3:…	Состояние 3: Аутентификация пройдена, соединение установлено

Злоумышленник фабрикует недействительные запросы аутентификации от подключенной клиентской станции, чтобы обманом заставить точку доступа выполнить разъединение подключенного клиента.

При осуществлении DoS-атаки данного типа фабрикуются недопустимые кадры запроса аутентификации (с плохими кодами службы или состояния аутентификации) от находящегося в Состоянии 3 подключенного клиента к точке доступа. После получения недействительных запросов аутентификации точка доступа обновляет клиента до состояния 1, что приводит к его отключению от беспроводной службы.

FATA-jack является одним из наиболее часто используемых инструментов для проведения подобной атаки. Данная модифицированная версия WLAN-jack передает на беспроводную станцию пакеты с ошибкой аутентификации вместе с кодом причины предыдущей ошибки аутентификации. Это происходит после подмены MAC-адреса точки доступа. Атака FATA-jack закрывает большинство активных соединений и иногда заставляет пользователя перезагружать станцию для продолжения нормальной работы.

Решение AirMagnet

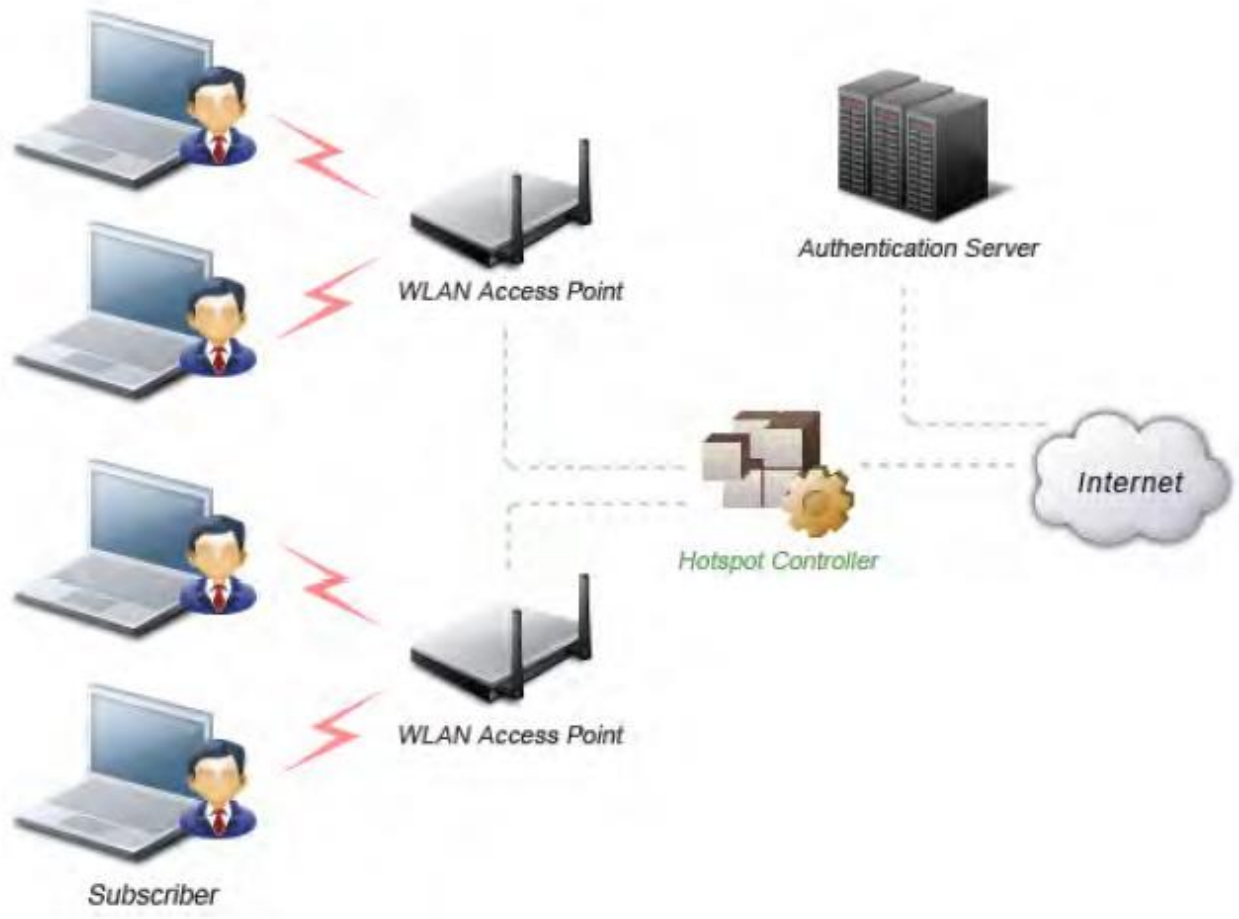
AirMagnet WiFi Analyzer обнаруживает использование FATA-jack, отслеживая поддельные MAC-адреса и ошибки аутентификации. Этот сигнал тревоги также может указывать на попытку проникновения. Когда

беспроводный клиент слишком много раз терпит неудачу при аутентификации соединения с точкой доступа, приложение AirMagnet WiFi Analyzer выдает этот сигнал тревоги, указывая на попытку потенциального злоумышленника взломать систему безопасности с помощью грубых компьютерных возможностей. Обратите внимание, что этот сигнал тревоги касается методов аутентификации 802.11 (открытая система, совместно используемый ключ и т.д.). Аутентификация на основе 802.1x и EAP отслеживается другими сигналами тревоги приложения AirMagnet WiFi Analyzer.

Device Vulnerable to Hotspot Attack Tools (Устройство уязвимо для инструментов атаки на публичные точки доступа)

Описание сигнала тревоги и возможные причины

Публичная точка доступа - это любое место, где доступ к сети Wi-Fi предоставляется широкой публике. Подобные точки доступа часто встречаются в аэропортах, отелях, кафе и других местах, где обычно собираются деловые люди. В наши дни это, вероятно, одна из самых важных услуг доступа к сети для деловых путешественников. Все, что требуется клиенту, это иметь ноутбук или карманное устройство с поддержкой беспроводной связи. Затем пользователь может подключиться к легитимной точке доступа и получить услугу. Большинство публичных точек доступа не требуют для подключения от пользователя какого-либо расширенного механизма аутентификации, кроме всплывающего окна веб-страницы для входа пользователя. Таким образом, критерий входа зависит только от того, оплатил ли подписчик абонентскую плату или нет. О среде публичных беспроводных точек доступа можно сказать, что здесь никому нельзя доверять. В наши дни по соображениям безопасности некоторые производители публичных точек доступа WLAN используют для проверки личности пользователя механизмы аутентификации 802.1x или выше.



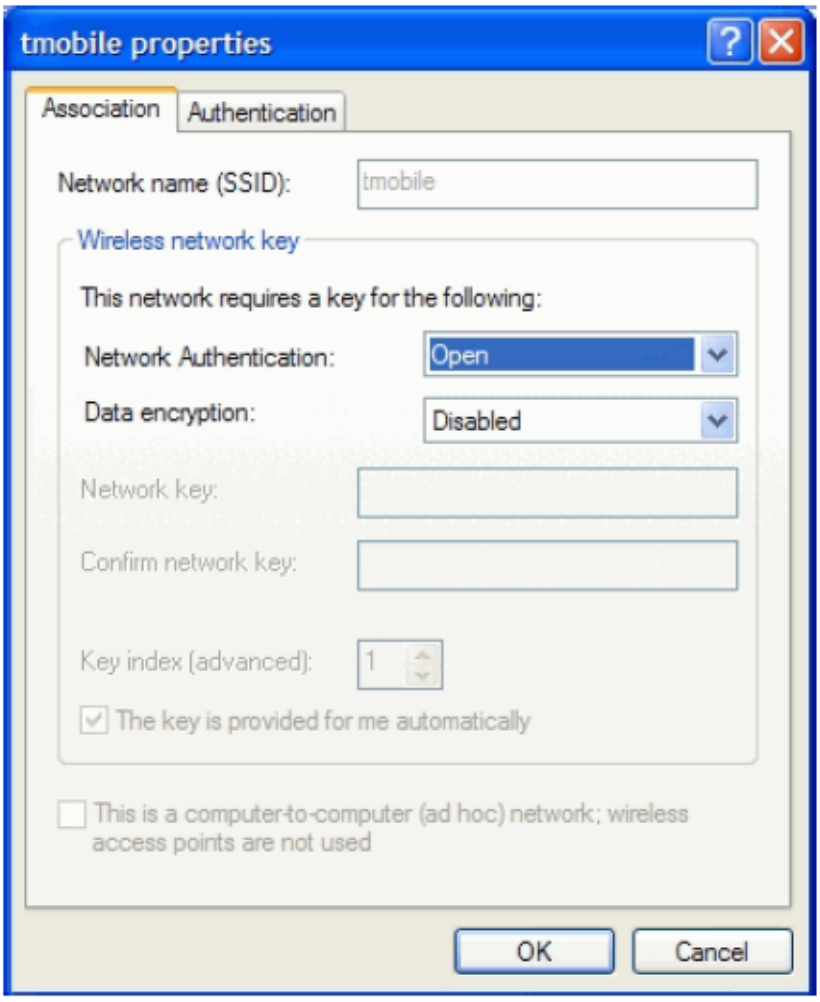
WLAN Access Point	Точка доступа к беспроводной локальной сети
Authentication Server	Сервер аутентификации
Hotspot Controller	Контроллер публичной точки доступа
Internet	Интернет
Subscriber	Подписчик

Основные компоненты сети WLAN с публичной точкой доступа

Четырьмя компонентами базовой сети с публичной точкой доступа являются:

- Подписчики публичной точки доступа: Это действительные пользователи с ноутбуком или портативным устройством с поддержкой беспроводной связи и действующим логином для доступа к сети с публичными точками доступа.
- Точки доступа WLAN: В зависимости от реализации сети с публичной точкой доступа это могут быть шлюзы SOHO или точки доступа корпоративного уровня.
- Контроллеры публичных точек доступа: Этот компонент имеет дело с аутентификацией пользователя, сбором информации для выставления счетов, отслеживанием времени использования, функциями фильтрации и т.д. Это может быть независимый компьютер или встроенный в саму точку доступа.
- Сервер аутентификации: Этот сервер содержит учетные данные подписчиков. Контроллер публичной точки доступа в большинстве случаев после получения учетных данных подписчиков проверяет их на сервере аутентификации.

У пользователей публичной точки доступа в настройках беспроводной сети Windows или в профиле карты WLAN будет настроен идентификатор SSID. Беспроводная карта будет отправлять зондирующие запросы с идентификатором SSID точки доступа. Это сделает клиентские станции уязвимыми для атак с помощью таких инструментов, как Airsnarf и Hotspotter.



Сетевые настройки для клиентского адаптера

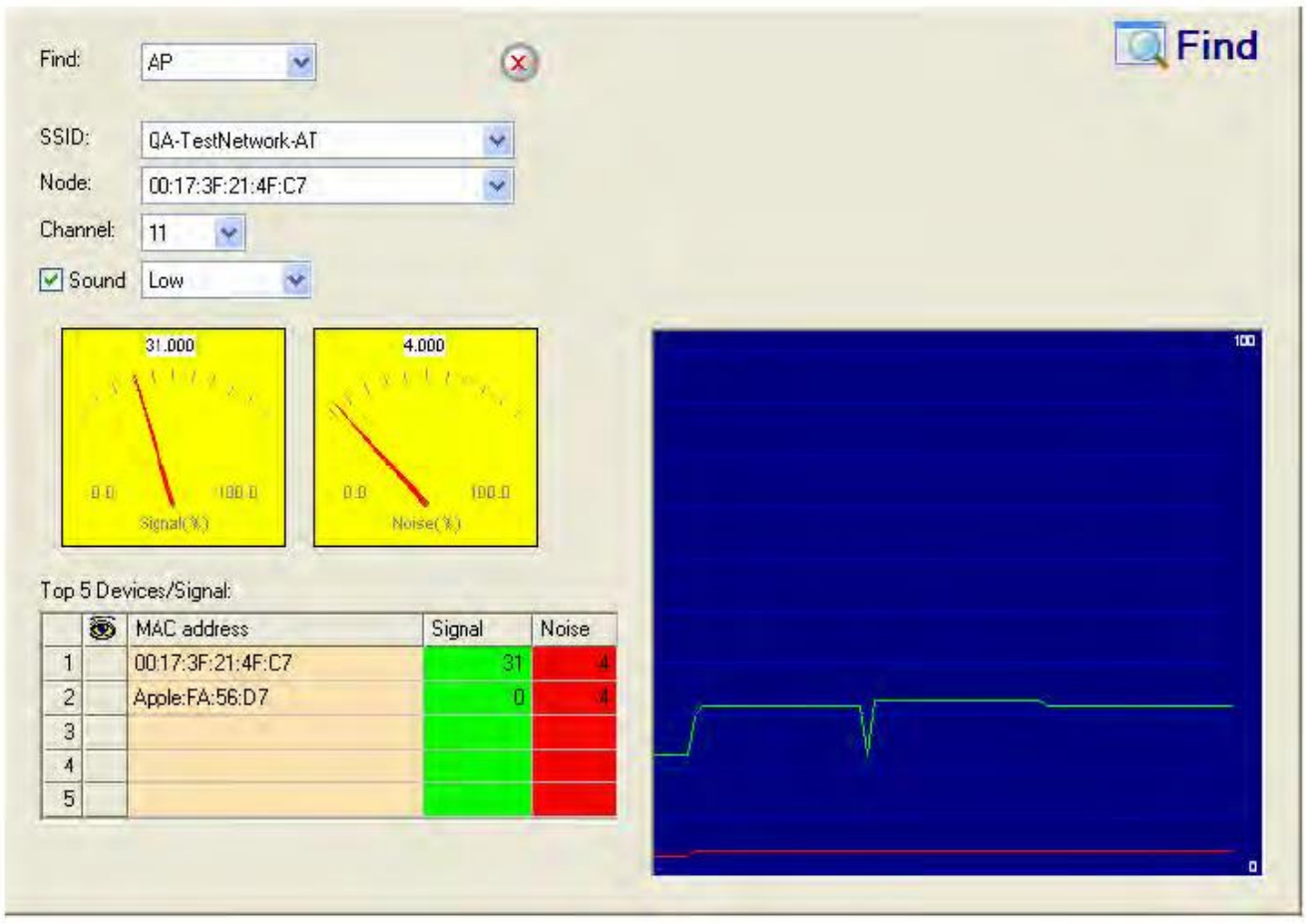
Наиболее часто используемые инструменты атаки автоматизируют метод проникновения в беспроводных клиентов, независимо от используемого механизма шифрования. Используя инструмент атаки, злоумышленник может пассивно контролировать беспроводную сеть на наличие кадров зондирующего запроса для определения идентификаторов SSID сетей клиентов Windows. После получения информации о предпочтительной сети злоумышленник может сравнить имя сети (SSID) с предоставленным списком часто используемых сетевых имен публичных точек доступа. Как только совпадение будет найдено, атакуемый клиент теперь будет действовать как точка доступа. Затем клиенты могут неосознанно

аутентифицироваться и соединиться с этой поддельной точкой доступа. Как только клиент подключится, инструмент атаки можно будет настроить для запуска команды, возможно, скрипта для запуска демона DHCP и другого сканирования новой жертвы. Одним из таких инструментов является Hotspotter.

Airsnarf - это утилита для настройки точки беспроводного доступа, показывающая, как хакер может украсть учетные данные пользователя (имя и пароль) из публичных точек беспроводного доступа. Основанный на скриптах оболочки инструмент Airsnarf создает публичную точку доступа с адаптивным порталом, куда пользователи вводят свои данные для входа. В файле конфигурации airsnarf можно настроить такие важные параметры, как информация о локальной сети, IP-адрес шлюза и SSID. Этот инструмент изначально передает очень сильный сигнал, который отсоединит беспроводных клиентов публичной точки доступа от авторизованной точки доступа, подключенной к сети Интернет. Беспроводные клиенты, предполагающие, что они были временно отключены от сети Интернет из-за какой-то неизвестной проблемы, попытаются снова войти в систему, чтобы возобновить свою работу. Ничего не подозревающие беспроводные клиенты, связывающиеся с точкой доступа Airsnarf, получают IP-адрес, DNS-адрес и IP-адрес шлюза от мошеннической точки доступа Airsnarf вместо легитимной точки доступа, установленной оператором. Пользователям будет показана веб-страница, запрашивающая имя пользователя и пароль, так как теперь запросы DNS решаются мошеннической точкой доступа Airsnarf. Введенные имена пользователей и пароли будут отправлены на адрес root@localhost. Имя пользователя и пароль можно будет использовать в любой другой точке доступа того же провайдера в любой точке страны, при этом пользователь не будет осознавать их мошенническое использование. Единственный случай, когда это может иметь небольшие последствия, это если пользователь точки доступа подключен по схеме с поминутной оплатой. Инструмент AirSnarf может быть загружен хакерами с http://airsnarf.shmoo.com/

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает клиентские станции, использующие идентификаторы SSID, настроенные для использования в среде Hotspot (публичных точек доступа). Чтобы избежать зондирования с использованием идентификатора SSID публичной точки доступа, приложение AirMagnet Wi-Fi Analyzer предлагает администратору использовать инструмент AirMagnet Find для поиска клиентов и принятия соответствующих мер.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Streaming Traffic from Wireless Device (Потоковый трафик с беспроводного устройства)

Описание сигнала тревоги и возможные причины

Спектр WLAN является общедоступной средой с ограничением полосы пропускания. Чтобы обеспечить достаточную доступность сети WLAN для всех клиентских устройств, использование полосы пропускания сети, будь то 802.11b со скоростью передачи 11 Мбит/с или 802.11a/g со скоростью передачи 54 Мбит/с, должно тщательно контролироваться для каждого канала и каждого устройства. Поэтому для администраторов очень важно следить за тем, чтобы вся полоса пропускания не использовалась одной клиентской станцией. Например, в корпоративных сетях могут возникнуть проблемы из-за того, что авторизованный пользователь загружает музыку или фильмы из Интернета, что приводит к снижению пропускной способности корпоративной сети. Музыка, потоковое видео, беспроводные камеры создают в беспроводной сети постоянный поток трафика.

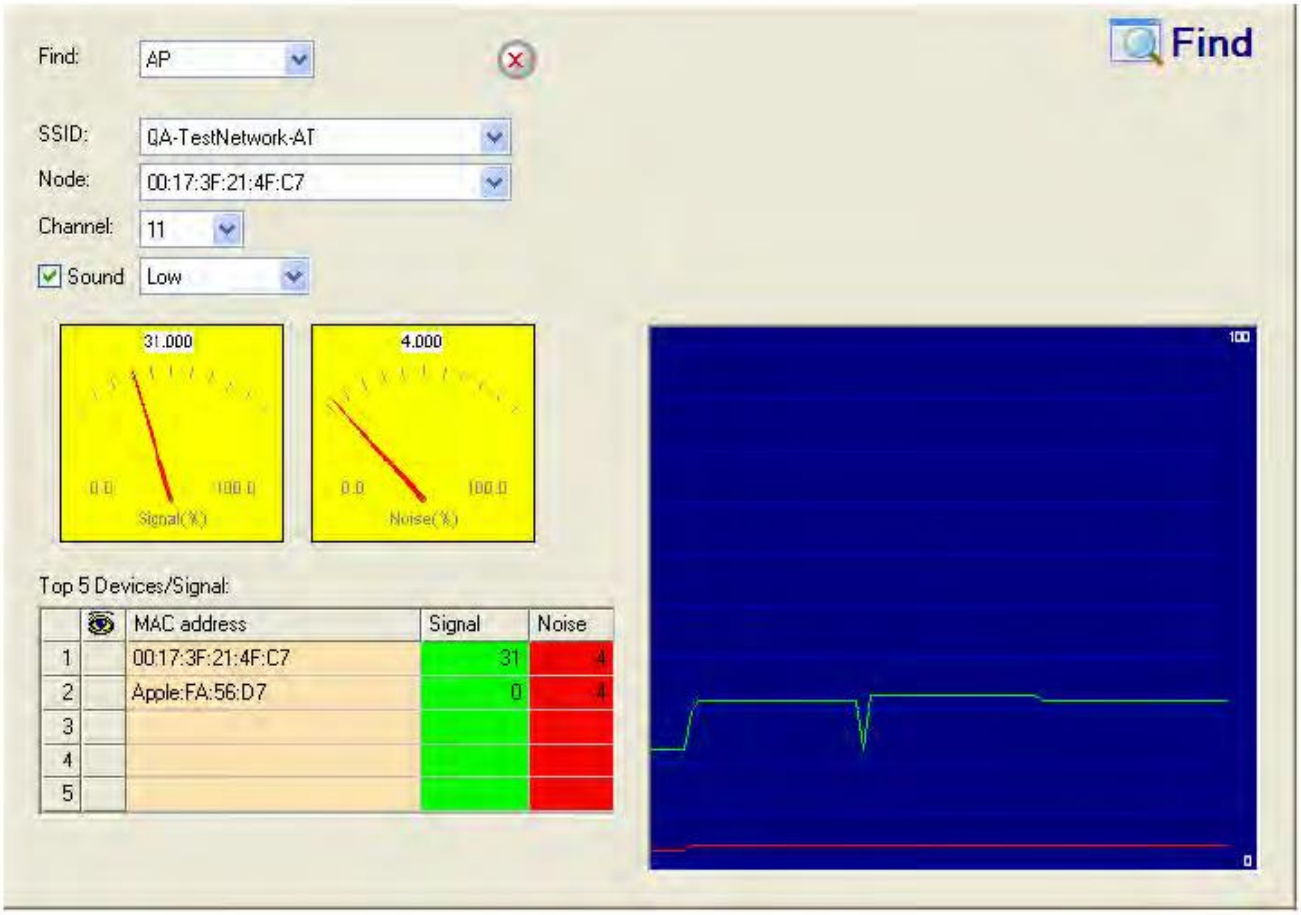
Потоковая передача с беспроводного ПК

Хотя потоковые приложения могут и не создавать критических проблем для проводных сетей, но способны оказывать существенное влияние на беспроводные сети, особенно на VoWLAN (Voice over WLAN).

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает беспроводные клиентские станции, которые в течение определенного промежутка времени постоянно передают данные по беспроводной сети. AirMagnet советует пользователю найти такие станции и предпринять необходимые меры для их отключения от беспроводной сети или попросить пользователя избегать использования беспроводной сети для подобных действий.

Как только осуществляющий потоковую передачу клиент идентифицирован приложением AirMagnet WiFi Analyzer и об этом передано соответствующее извещение, администратор WLAN может использовать инструмент FIND (Найти) для определения местоположения потокового устройства.

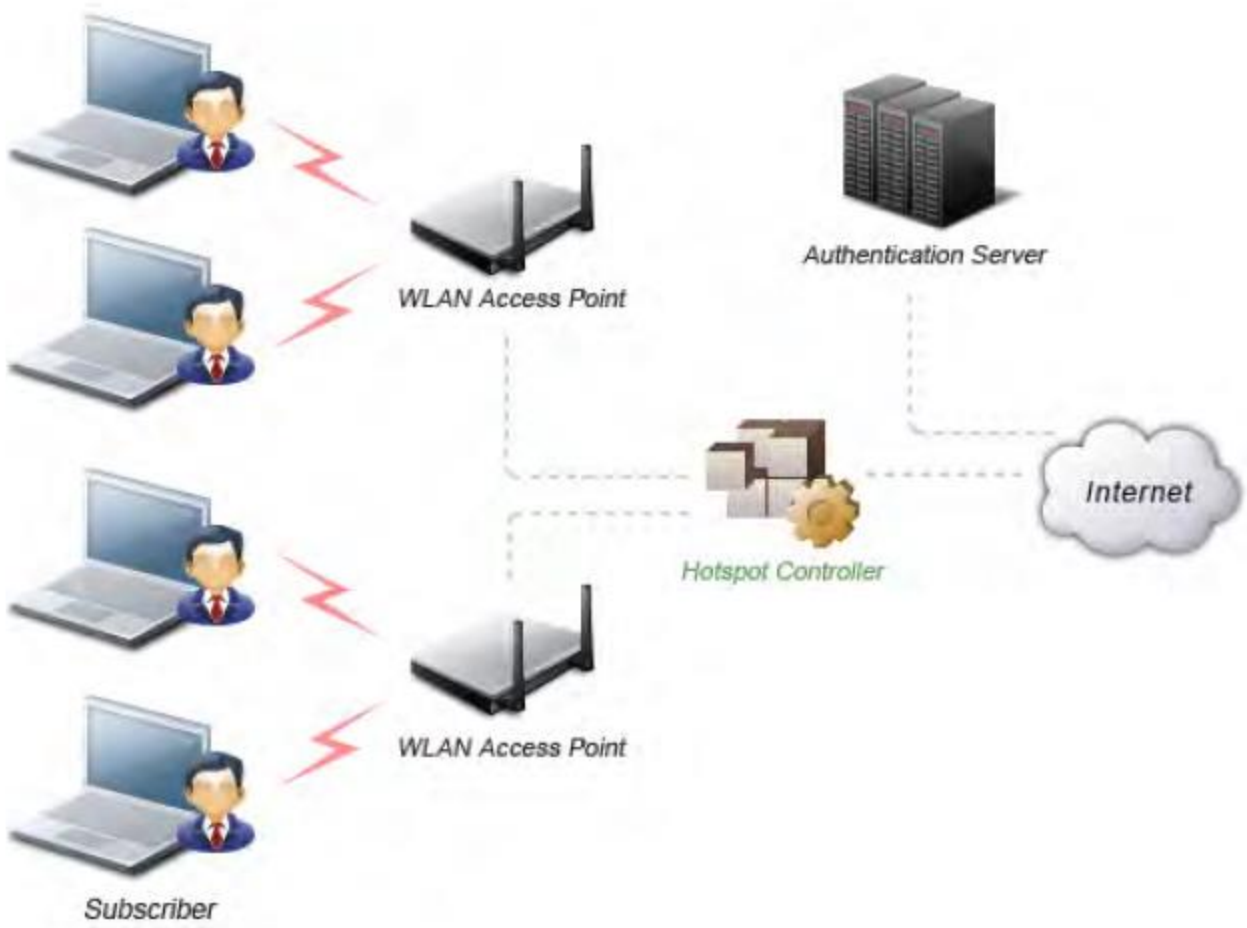


Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Hotspotter Tool Detected (Potential Wireless Phishing) (Обнаружен инструмент Hotspotter (потенциальный беспроводной фишинг))

Описание сигнала тревоги и возможные причины

Публичная точка доступа - это любое место, где доступ к сети Wi-Fi предоставляется широкой публике. Подобные точки доступа часто встречаются в аэропортах, отелях, кафе и других местах, где обычно собираются деловые люди. В наши дни это, вероятно, одна из самых важных услуг доступа к сети для деловых путешественников. Все, что требуется клиенту, это иметь ноутбук или карманное устройство с поддержкой беспроводной связи. Затем пользователь может подключиться к легитимной точке доступа и получить услугу. Большинство публичных точек доступа не требуют для подключения какого-либо расширенного механизма аутентификации, кроме всплывающего окна веб-страницы для входа пользователя. Таким образом, критерий входа зависит только от того, оплатил ли подписчик абонентскую плату или нет. О среде публичных беспроводных точек доступа можно сказать, что здесь никому нельзя доверять. В наши дни по соображениям безопасности некоторые производители публичных точек доступа WLAN используют для проверки личности пользователя механизмы аутентификации 802.1x или выше.



WLAN Access Point	Точка доступа к беспроводной локальной сети
Authentication Server	Сервер аутентификации
Hotspot Controller	Контроллер публичной точки доступа
Internet	Интернет
Subscriber	Подписчик

Основные компоненты сети WLAN с публичной точкой доступа

Четырьмя компонентами базовой сети с публичной точкой доступа являются:

- Подписчики публичной точки доступа: Это легитимные пользователи с ноутбуком или портативным устройством с поддержкой беспроводной связи и действующим логином для доступа к сети с публичной точкой доступа.

- Точки доступа WLAN: В зависимости от реализации сети с публичной точкой доступа это могут быть шлюзы SOHO или точки доступа корпоративного уровня.
- Контроллеры публичных точек доступа: Этот компонент имеет дело с аутентификацией пользователя, сбором информации для выставления счетов, отслеживанием времени использования, функциями фильтрации и т.д. Это может быть независимый компьютер или устройство, встроенное в саму точку доступа.
- Сервер аутентификации: Этот сервер содержит учетные данные подписчиков. Контроллер публичной точки доступа в большинстве случаев после получения учетных данных подписчиков проверяет их на сервере аутентификации.

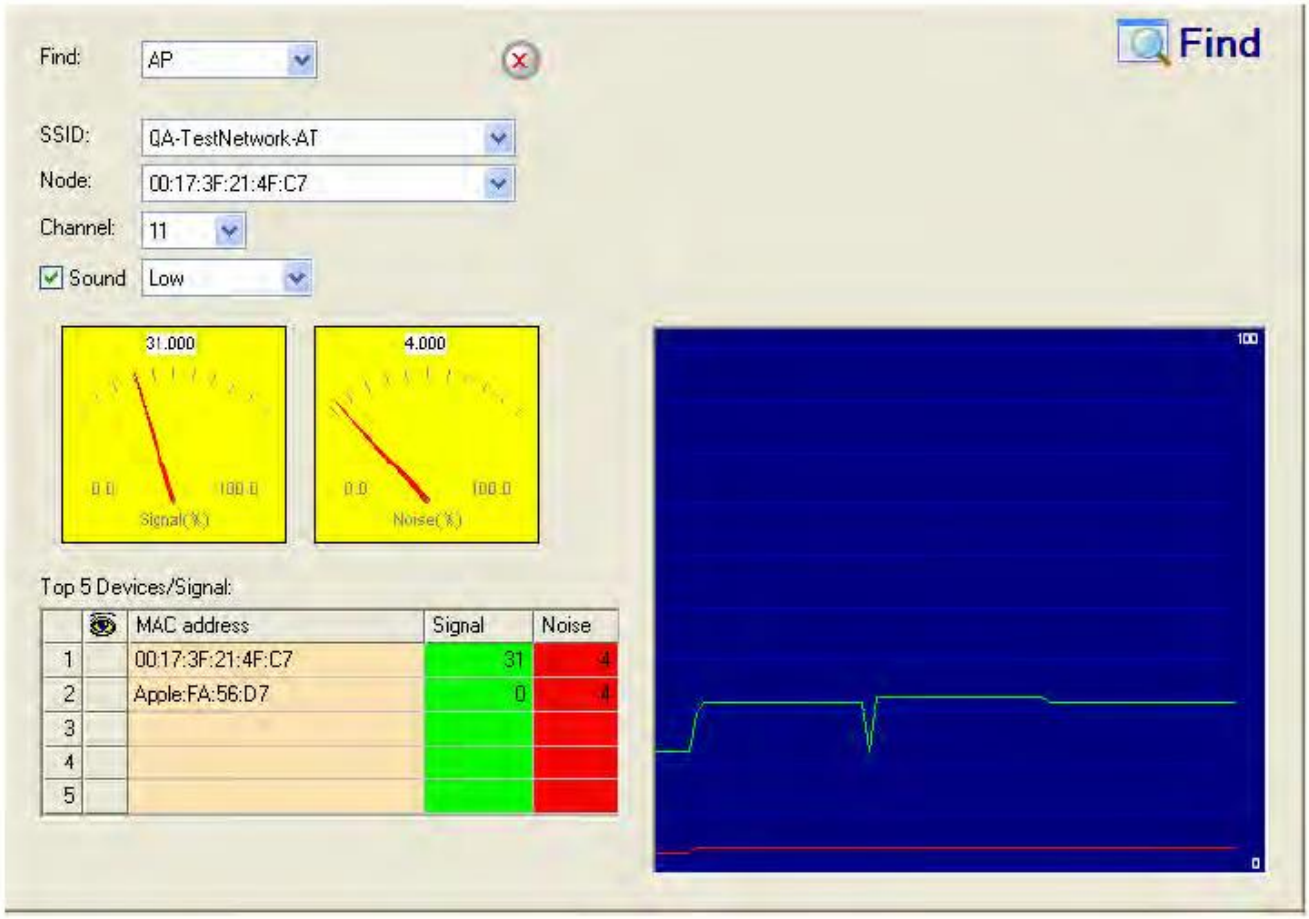
Hotspotter автоматизирует метод проникновения в беспроводных клиентов, независимо от используемого механизма шифрования. Используя инструмент Hotspotter, злоумышленник может пассивно контролировать беспроводную сеть на наличие кадров зондирующего запроса для определения идентификаторов SSID сетей клиентов Windows.
После получения информации о предпочтительной сети злоумышленник может сравнить имя сети (SSID) с предоставленным списком часто используемых сетевых имен публичных точек доступа. Как только совпадение будет найдено, клиент Hotspotter будет действовать как точка доступа. Затем клиенты могут неосознанно аутентифицироваться и соединиться с этой поддельной точкой доступа.

Как только клиент подключится, инструмент Hotspotter можно будет настроить для запуска команды, возможно, скрипта для запуска демона DHCP и другого сканирования новой жертвы.

Клиенты подвергаются такому виду атак не только в среде точки доступа, но и при работе в разных средах (дома и в офисе), когда они все еще настроены на включение SSID публичной точки доступа в настройки беспроводного подключения Windows. Клиенты будут отправлять зондирующие запросы, используя этот идентификатор SSID, и станут уязвимыми для инструмента злоумышленника.

Решение AirMagnet

После того, как неавторизованная точка доступа будет идентифицирована и о ней сообщит приложение AirMagnet WiFi Analyzer, администратор WLAN сможет использовать инструмент FIND (Найти) для определения местонахождения устройства злоумышленника.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

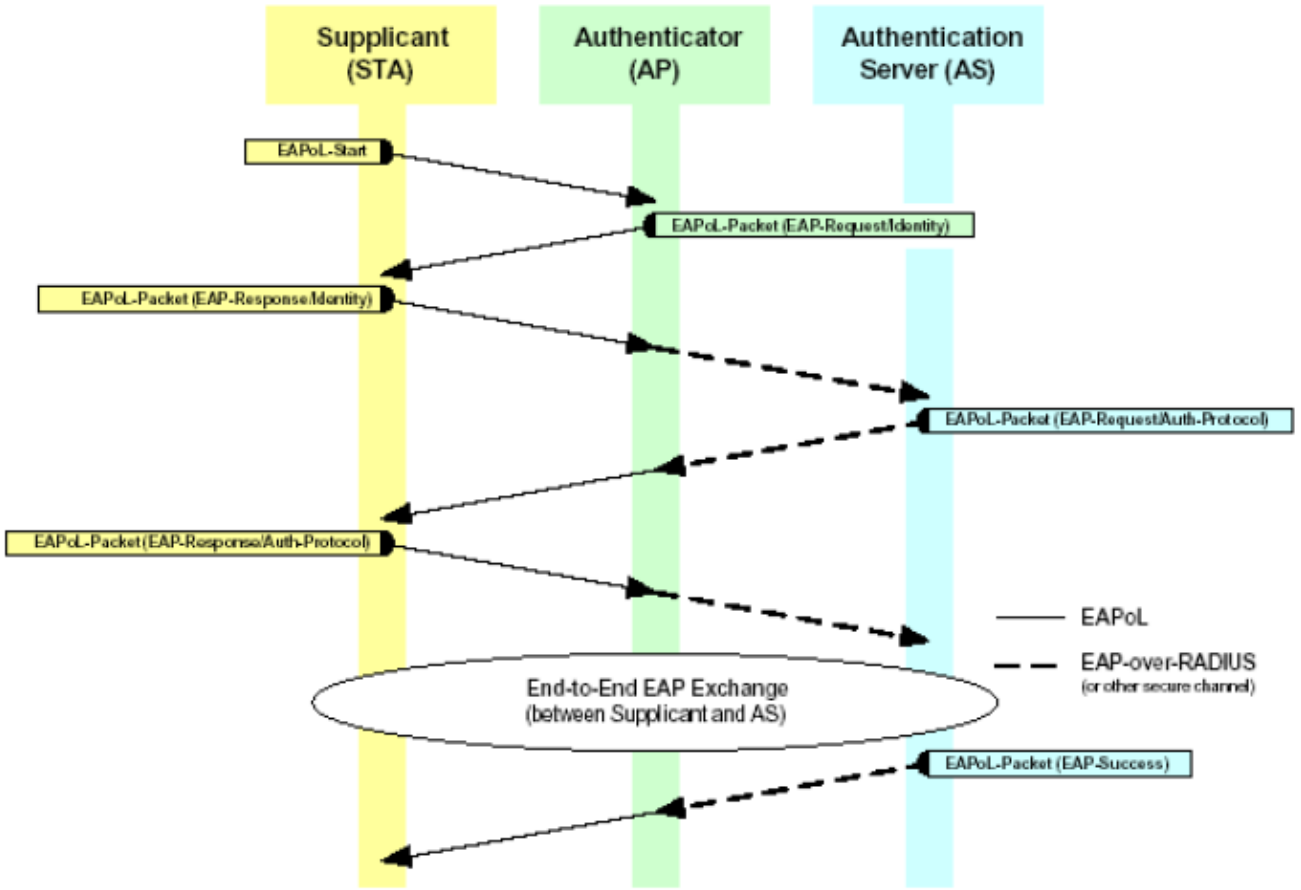
Device Unprotected by IEEE 802.11i/AES (Устройство не защищено IEEE 802.11i/AES)

Описание сигнала тревоги и возможные причины

Новый стандарт 802.11i обеспечивает две из трех критически важных возможностей сетевой безопасности - аутентификацию и конфиденциальность. AirMagnet Enterprise предупреждает об обнаружении устройств, не использующих стандарт IEEE 802.11i. Устройства, которые не используют этот стандарт безопасности, могут быть уязвимы для различных атак, ставящих под угрозу безопасность корпоративной сети.

Когда был ратифицирован стандарт IEEE 802.11, в нем в качестве стандарта безопасности предлагалась реализация 64-битного ключа WEP. Со временем производители оборудования увеличили это значение до 128-битных ключей и т.д. В некоторых случаях даже объявлялось, что используются ключи WEP длиной до 256 бит. С тех пор было доказано, что статический WEP несовершенен с точки зрения аутентификации, шифрования и проверки целостности. Вскоре альянс Wi-Fi осознал важность создания альтернативы стандарту WEP. Стандарт IEEE 802.11i был введен для смягчения всех проблем безопасности, которые преследовали беспроводные сети в корпоративной среде. Этот стандарт создает надежные защищенные сети (RSN – Robust Secure Networks).

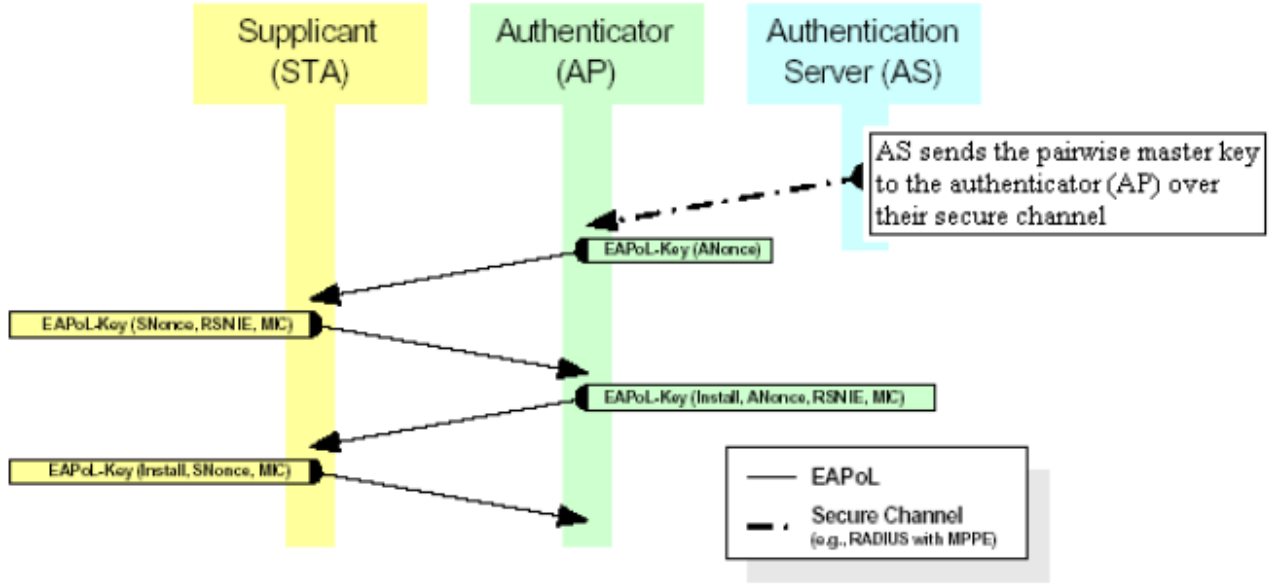
Поскольку стандарт 802.11i не будет ратифицирован вовремя, Wi-Fi Alliance создал подмножество стандарта IEEE 802.11i под названием Wi-Fi Protected Access (WPA). WPA/802.11i реализует 802.1x для аутентификации пользователей и распределения ключей. 802.1x используется с различными типами протоколов расширенной аутентификации (Extensible Authentication Protocol), такими как LEAP, TLS, TTLS, EAP-FAST и PEAP, для реализации механизма аутентификации и шифрования. Стандарт IEEE 802.11i оставляет выбор схемы аутентификации за пользователем.



Supplicant (STA)	Проситель (станция)
Authenticator (AP)	Аутентификатор (точка доступа)
Authentication Server (AS)	Сервер аутентификации
EAPoL– Start	EAPoL – Старт
EAPoL-Packet (EAP-Request/Identity)	Пакет EAPoL (EAP-Запрос/Идентификатор)
EAPoL-Packet (EAP-Response/Identity)	Пакет EAPoL (EAP-Ответ/Идентификатор)
EAPoL-Packet (EAP-Request/Auth-Protocol)	Пакет EAPoL (EAP-Запрос/Протокол аутентификации)
EAPoL-Packet (EAP- Response/Auth-Protocol)	Пакет EAPoL (EAP-Ответ/Протокол аутентификации)
End-to-End EAP Exchange…	Сквозной обмен EAP (между просителем и сервером аутентификации)
EAP-over-RADIUS…	EAP через RADIUS (или другой безопасный канал)
EAPoL-Packet (EAP-Success)	Пакет EAPoL (EAP-Успешно)

Структура 802.1x обеспечивает централизованную аутентификацию пользователей и управление ключами шифрования.

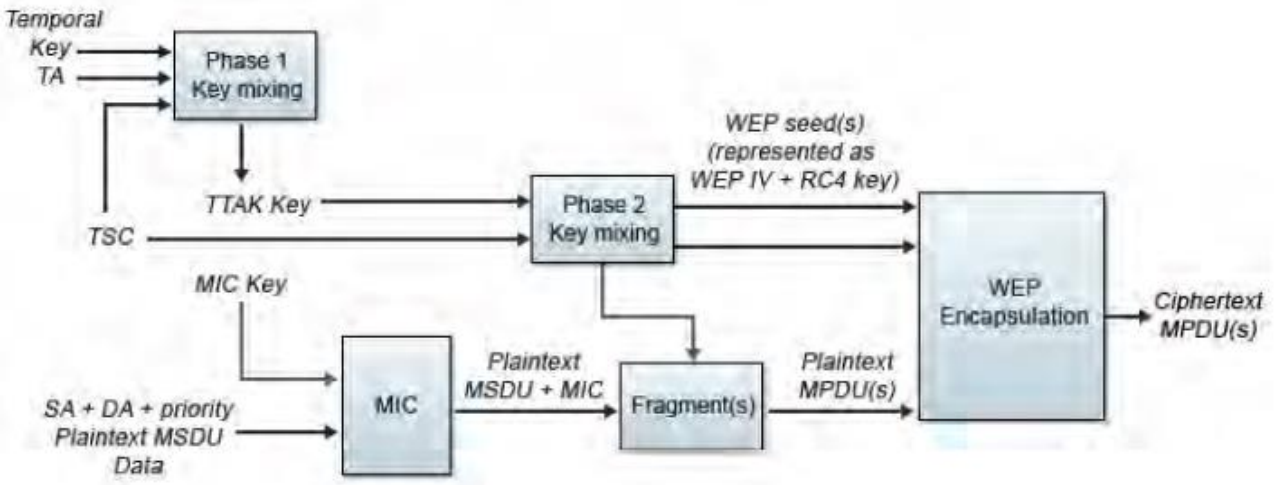
Стандарт IEEE 802.11i обеспечивает механизм предварительного совместно используемого ключа (PSK) и схемы управления ключами на основе сервера 802.1x. Для безопасного и динамического распределения ключей сеанса (PMK/Pairwise Master Key - парный главный ключ) механизму на основе сервера требуется такой сервер аутентификации, как RADIUS. Когда вместо 802.1x используется PSK, парольная фраза PSK преобразуется с помощью формулы в 256-битное значение, необходимое для парного главного ключа. В режиме PSK для управления ключами шифрования используется 4-стороннее установление связи, определенное стандартом 802.11i, без обмена EAP. Поскольку отсутствует сервер RADIUS и методы EAP (EAP-TLS, LEAP), режим PSK менее безопасен.



Supplicant (STA)	Проситель (станция)
Authenticator (AP)	Аутентификатор (точка доступа)
Authentication Server (AS)	Сервер аутентификации
AS sends the pairwise master key…	Сервер аутентификации передает парный главный ключ аутентификатору (точке доступа) по своему безопасному каналу
Key	Ключ
Secure Channel…	Безопасный канал (например, RADIUS с MPPE)

Для работы в режиме предварительного совместно используемого ключа 4-сторонний процесс установления связи выполняет обмен ключами (точка доступа аутентификатора и сервер аутентификации находятся на устройстве точки доступа)

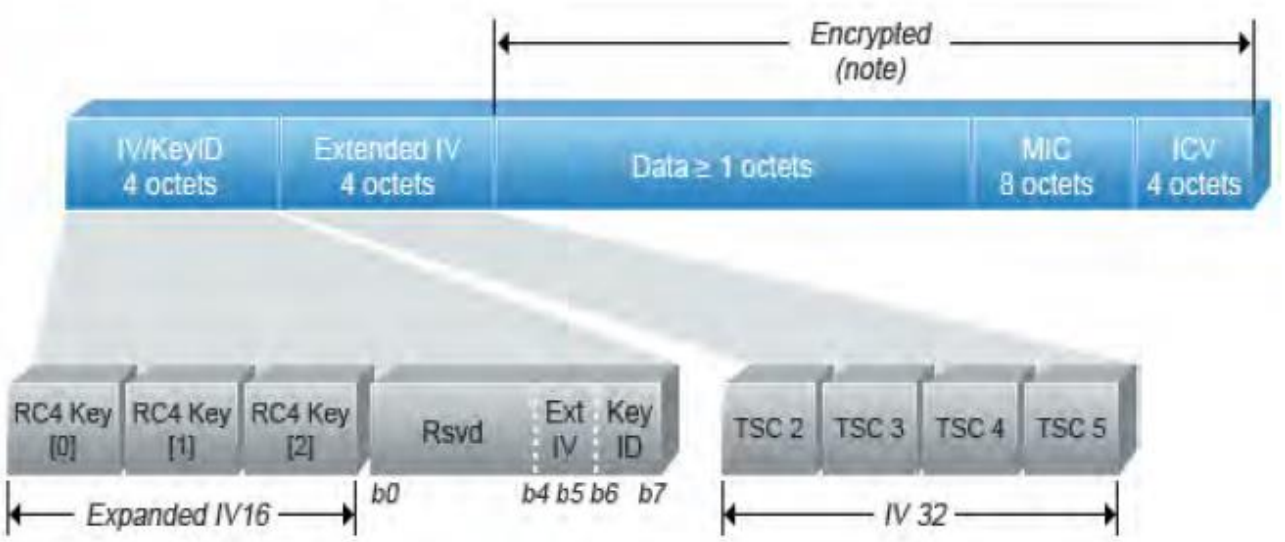
В IEEE 802.11i определены два стандарта шифрования: протокол TKIP (ограниченной по времени целостности ключа) и протокол Advanced Encryption Standard-Counter Mode-CBC MAC. Зашифрованный с помощью TKIP и MIC трафик WLAN предотвращает подделку пакетов и атаку повторного воспроизведения. Что наиболее важно, протокол TKIP невосприимчив к уязвимости, вызванной статическим ключом WEP, и атакам, возникающим в результате повторного использования ключа. Наряду с MIC, протокол TKIP также обеспечивает смешивание ключей для каждого пакета, что помогает предотвратить множество атак с использованием потоков ключей.



Temporal Key	Временный ключ
Phase 1 Key mixing	Этап 1 Микширование ключей
TTAK Key	Ключ TTAK

Phase 2 Key mixing	Этап 2 Микширование ключей
WEP seed(s)…	Сид(ы) WEP (представлен как WEP IV + ключ RC4)
MIC Key	Ключ MIC
SA+DA+priority…	SA+DA+ приоритет Открытый текст MSDU Данные
Plaintext MSDU+MIC	Открытый текст MSDU+MIC
Fragment(s)	Фрагмент(ы)
Plaintext MPDU	Открытый текст MPDU
WEP Encapsulation	Инкапсуляция WEP
Ciphertext MPDU(s)	Зашифрованный текст MPDU

Алгоритм шифрования TKIP и MIC устраняет слабые места статического WEP, а также предотвращает подделку пакетов и атаку путем повтора перехваченных данных.

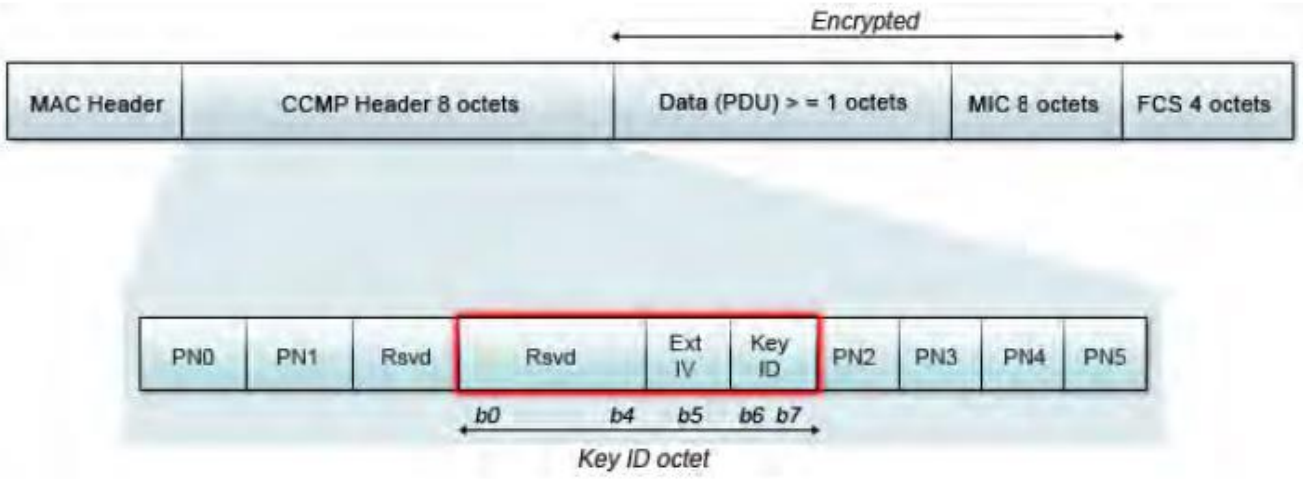


Encrypted (note)	Зашифрованная часть
IV/KeyID 4 octets	IV/KeyID 4 октета
Extended IV 4 octets	Увеличенный IV 4 октета
Data ≥ 1 octet	Данные ≥ 1 октет
MIC 8 octets	MIC 8 октетов
ICV 4 octets	ICV 4 октета
Key	Ключ
Expanded IV 16	Расширенный IV 16

Кадры с шифрованием TKIP и MIC расширяют исходные данные на 20 байт для более надежного шифрования и проверки целостности.

Реализация AES-CCMP является обязательной для стандарта IEEE 802.11i. Стандарт IEEE поддерживает только 128-битное шифрование AES. Поскольку шифрование AES должно работать с 128-битными блоками, CCMP обеспечивает заполнение, необходимое для увеличения битового размера блока данных. Это заполнение добавляется перед шифрованием и отбрасывается после дешифрования.

Режим AES-CCMP обеспечивает аутентификацию и шифрование с использованием блочного шифра AES. CCMP представляет собой комбинацию шифрования в режиме счетчика (CTR) для обеспечения конфиденциальности данных и аутентификации с использованием кода CBC-MAC (построение аутентификационного кода сообщения из блочного шифра) для обеспечения безопасности аутентификации и шифрования для каждого обрабатываемого блока данных. CCMP вычисляет CBC-MAC по длине заголовка IEEE 802.11, выбранным частям заголовка IEEE 802.11 MAC Payload Data Unit (MPDU) и открытым текстовым данным MPDU, тогда как старый механизм IEEE 802.11 WEP не обеспечивает защиты заголовка MPDU. Во-вторых, как шифрование, так и дешифрование CCMP использует только функцию прямого блочного шифрования AES, что приводит к значительной экономии кода и размера оборудования.



Encrypted	Зашифровано
MAC Header	Заголовок MAC
CCMP Header 8 octets	Заголовок CCMP 8 октетов
Data (PDU) >= 1 octets	Данные (PDU) >= 1 октет
MIC 8 octets	MIC 8 октетов
FCS 4 octets	FCS 4 октета
Key ID octet	Октет идентификатора ключа

CCMP MPDU

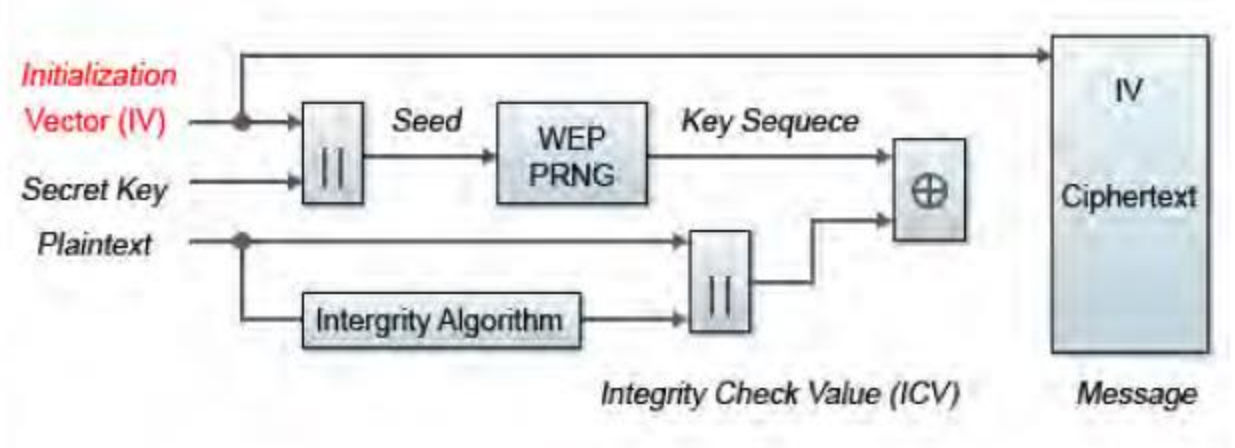
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer предупреждает об обнаружении устройств, которые не используют стандарт IEEE 802.11i и, возможно, ставят под угрозу безопасность беспроводной сети. Приложение AirMagnet WiFi Analyzer рекомендует пользователю предпринять соответствующие шаги, чтобы избежать любых дыр безопасности в сети и обновить инфраструктуру беспроводной сети и устройства для использования более безопасного стандарта IEEE 802.11i.

Fast WEP Crack (ARP Replay) Detected (Обнаружен быстрый взлом WEP (ARP Replay))

Описание сигнала тревоги и возможные причины

Хорошо известно, что использующее для шифрования статический ключ WEP устройство WLAN уязвимо для различных атак взлома WEP (Обратитесь к документу «Weaknesses in the Key Scheduling Algorithm of RC4 – I» (Слабые стороны алгоритма планирования ключей RC4 – I), авторы Scott Fluhrer, Itsik Mantin и Adi Shamir (Скотт Флурер, Ицик Мантин и Ади Шамир)).



Initialization Vector (IV)	Вектор инициализации (IV)
Seed	Сид
Key Sequence	Последовательность ключа
Secret Key	Секретный ключ
Plaintext	Открытый текст
Integrity Algorithm	Алгоритм целостности
Ciphertext	Зашифрованный текст
Integrity Check Value (ICV)	Значение проверки целостности (ICV)
Message	Сообщение

Блок-схема процесса шифрования WEP

Взлом злоумышленником секретного ключа WEP приводит к отсутствию защиты шифрованием, что ставит под угрозу конфиденциальность данных. Ключ WEP, который в большинстве случаев является 64-битным или 128-битным (некоторые производители также предлагают 152-битное шифрование), состоит из секретного ключа, сконфигурированного пользователем, соединенного с 24-битным IV (вектором инициализации). IV определяется передающей станцией. Когда ключ IV повторно используется часто или в последовательных кадрах, это увеличивает вероятность восстановления секретного ключа хакерами, проникающими в беспроводную сеть.

Наиболее важным фактором при любой атаке на ключ WEP является его размер. Для 64-битных ключей WEP должно быть достаточно около 150 000 уникальных IV, а для 128-битных ключей WEP от 500 000 до миллиона уникальных IV. На тот случай, когда трафика недостаточно, хакеры придумали уникальный способ генерации достаточного трафика для выполнения такой атаки. Эта атака повторной передачи перехваченных кадров, основанная на пакетах arp-запроса. Такие пакеты имеют фиксированную длину и могут быть легко обнаружены. Захватив один допустимый пакет arp-запроса и повторно отправляя его снова и снова, злоумышленник заставляет другой хост отвечать зашифрованными ответами, тем самым предоставляя новые и, возможно, слабые IV.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer предупреждает о слабой реализации WEP и для устранения проблемы с использованием вектора инициализации (IV) рекомендует обновить прошивку устройства, запросив ее у производителя устройства. В идеале корпоративную сеть WLAN можно защитить от уязвимости WEP с помощью шифрования TKIP (Temporal Key Integrity Protocol – Протокол ограниченной по времени целостности ключа), которое поддерживается большей частью беспроводного оборудования корпоративного уровня. Устройства с поддержкой TKIP не подвержены атаке по ключу WEP.

AP Overloaded by Voice Traffic (Точка доступа перегружена голосовым трафиком)

Описание сигнала тревоги и возможные причины

Точка доступа WLAN имеет ограниченные ресурсы и поэтому может обслуживать только ограниченное количество клиентов. При достижении предела дополнительные клиенты могут обнаружить, что их запросы на обслуживание отклонены, а у существующих клиентов может снизиться производительность. Это неприемлемо в среде, где используются телефоны VoWLAN. Данное ограничение следует учитывать при развертывании оборудования и проектировании предоставления услуг WLAN. Важно помнить, что обычно одна точка доступа, поддерживающая трафик VoWLAN, используется для предоставления голосовых услуг 6 - 8 пользователям телефонов, и что проблемы с голосом кардинально отличаются от тех, которые возникают при обычной передаче данных в беспроводной сети. По мере роста числа пользователей уже после развертывания сети существующему оборудованию может стать все труднее поддерживать постоянное обслуживание. Эта ситуация требует непрерывного контроля на случай возникновения проблем.

Точка доступа перегружена телефонами с VoWLAN

В определенных сценариях клиенты VoWLAN в роуминге могут обнаружить точку доступа с лучшим приемом сигнала и попытаться подключиться к ней. Однако если эта конкретная точка доступа перегружена другими клиентами или имеет высокое использование пропускной способности, вызовы VoWLAN могут периодически прерываться и давать ощущение снижения производительности сети.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer контролирует рабочую нагрузку точки доступа, отслеживая ее активных клиентов VoWLAN. Систему можно настроить на подачу сигнала тревоги в зависимости от количества телефонов, поддерживаемых каждой точкой доступа в вашей сети. Это позволит быть уверенным в том, что вы своевременно узнаете, когда данная точка доступа не сможет обрабатывать больше соединений. В этом случае для удовлетворения растущего спроса может потребоваться добавить к существующей инфраструктуре дополнительные точки доступа. В качестве альтернативы, если это возможно, можно также попытаться уменьшить рабочую нагрузку, исключив некоторые ненужные соединения. Используйте экран Infrastructure (Инфраструктура), чтобы определить, какие устройства

подключаются к данной точке доступа, и, используя эти знания, выберите устройства (если таковые имеются), которые можно удалить из вашей сети.

Channel Overloaded by Voice Traffic (Канал перегружен голосовым трафиком)

Описание сигнала тревоги и возможные причины

Согласно стандарту IEEE 802.11e для QoS (Качество обслуживания) базовый набор услуг QoS (QBSS) представляет собой набор базовых служб (BSS), который поддерживает приложения LAN с требованиями к качеству обслуживания (QoS), предоставляя средство QoS для связи через беспроводную среду. С введением стандарта IEEE 802.11e было сделано несколько изменений в формате исходных кадров 802.11. Среди множества других кадров, кадр маяка и кадр ответа на зондирование теперь включают новые записи, если информация относится к качеству обслуживания (QoS).

Использование	Порядок	Информация	Примечание
Всегда присутствует	1	Метка времени	
	2	Интервал сигнала маяка	
	3	Информация о возможностях	
	4	Идентификатор SSID	
	5	Поддерживаемые скорости передачи	
Присутствует, если требуется для типа PHY, типа BBS или активного координатора точек (смотрите примечания)	6	FH Parameter Set	Информационный элемент FH Parameter Set присутствует в кадрах маяка, генерируемых станциями, использующими на физическом уровне скачкообразную перестройку частоты.
	7	DS Parameter Set	Информационный элемент DS Parameter Set присутствует в кадрах маяка, генерируемых станциями, использующими на физическом уровне прямую последовательность.
	8	CF Parameter Set	Информационный элемент CF Parameter Set присутствует в кадрах маяка, генерируемых точками доступа с активным PC или точками доступа QAP.
	9	IBSS Parameter Set	Информационный элемент IBSS Parameter Set присутствует только в кадрах маяка, генерируемых станциями в IBSS.
	10	TIM	Информационный элемент TIM присутствует только в кадрах маяка, генерируемых точками доступа в QAP.
Несколько регуляторных доменов	11	Информация о стране	Информационный элемент Country должен присутствовать, когда dot11MultipleDomainCapabilityEnabled является истиной.
	12	Параметры FH	Когда dot11MultipleDomainCapabilityEnabled является истиной, могут быть включены параметры FH, как задано в пункте 7.3.2.13.
	13	Таблица шаблонов FH	Когда dot11MultipleDomainCapabilityEnabled является истиной, может быть включена информация таблицы шаблонов FH, как задано в пункте 7.3.2.13.
QBSS	14	QBSS Load	Информационный элемент QBSS Load присутствует только в кадрах маяка, генерируемых QAP.
	15	QOS Parameter Set	Информационный элемент QOS Parameter Set присутствует только в кадрах маяка, генерируемых QAP.

Формат кадра маяка, предложенный стандартом IEEE 802.11e

Использование	Порядок	Информация	Примечание
Всегда присутствует	1	Метка времени	
	2	Интервал сигнала маяка	
	3	Информация о возможностях	
	4	Идентификатор SSID	
	5	Поддерживаемые скорости передачи	
Присутствует, если требуется для типа PHY, типа BBS или активного координатора точек (смотрите примечания)	6	FH Parameter Set	Информационный элемент FH Parameter Set присутствует в кадрах ответа на зондирование, генерируемых станциями, использующими на физическом уровне скачкообразную перестройку частоты.
	7	DS Parameter Set	Информационный элемент DS Parameter Set присутствует в кадрах ответа на зондирование, генерируемых станциями, использующими на физическом уровне прямую последовательность.
	8	CF Parameter Set	Информационный элемент CF Parameter Set присутствует в кадрах маяка, генерируемых точками доступа с активным PC или точками доступа QAP.
	9	IBSS Parameter Set	Информационный элемент IBSS Parameter Set присутствует только в кадрах ответа на зондирование, генерируемых станциями в IBSS.
Несколько регуляторных доменов	10	Информация о стране	Включен, если dot11MultipleDomainCapabilityEnabled является истиной.
	11	Параметры FH	Когда dot11MultipleDomainCapabilityEnabled является истиной, могут быть включены параметры FH, как задано в пункте 7.3.2.13.
	12	Таблица шаблонов FH	Когда dot11MultipleDomainCapabilityEnabled является истиной, может быть включена информация таблицы шаблонов FH, как задано в пункте 7.3.2.13.
	13-n	Элементы запрошенной информации	Элементы, запрошенные с помощью элемента запроса информации кадра зондирующего запроса.
QBSS всегда присутствует	10	QBSS Load	Информационный элемент QBSS Load присутствует только в кадрах зондирующего запроса, генерируемых QAP.
	11	Error Statistics	Информационный элемент Error Statistics присутствует только в кадрах зондирующего запроса, генерируемых QSTA в QBSS.
QBSS присутствует, если необходимо	12	Listen Epoch	Информационный элемент Listen Epoch присутствует только в кадрах зондирующего запроса, генерируемых QSTA в QBSS, имеющих назначенное время прослушивания.
	13	Extended Capabilities	Информационный элемент Extended Capabilities присутствует только в кадрах зондирующего запроса, генерируемых QSTA с информационным битом Capabilities 15 = 1.

Формат кадра ответа на зондирование, предложенный стандартом IEEE 802.11e

Оба эти кадра включают элемент QBSS Load. Элемент QBSS Load содержит информацию о текущем количестве станций и уровнях трафика в QBSS.

Идентификатор элемента	Длина	Счетчик станций	Использование канала	Доступная емкость подключения

Формат элемента Load

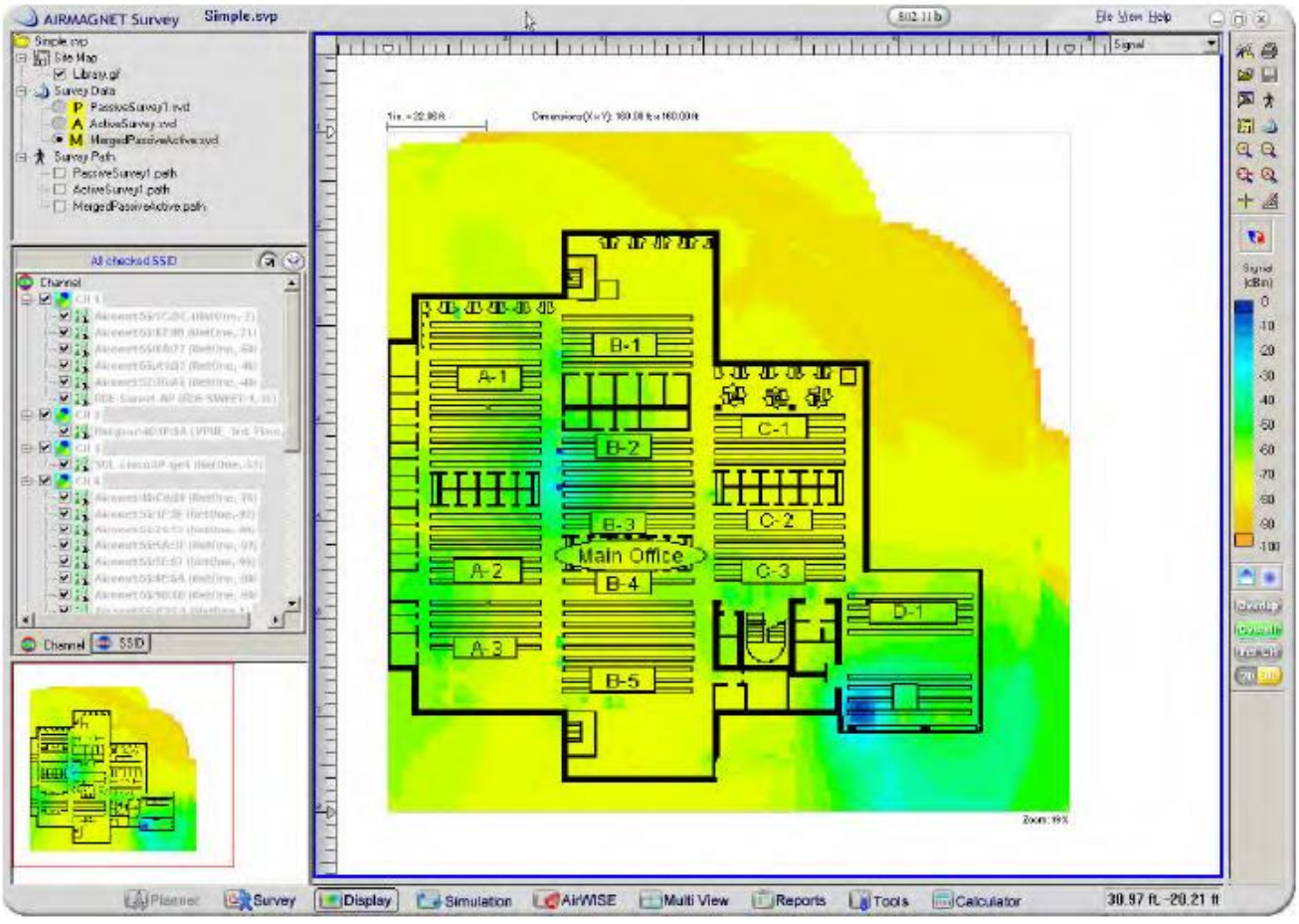
В поле использования канала (Channel Utilization) указывается часть доступной полосы пропускания беспроводной среды, которая в настоящее время используется для транспортировки трафика в этом QBSS.

Решение AirMagnet

AirMagnet рекомендует поддерживать использование канала на минимуме. Одним из самых простых способов сделать это является уменьшение количества клиентских устройств, которые могут обращаться к одной точке доступа. Другим широко используемым вариантом является плотное развертывание точек доступа, процедура, при которой точки доступа устанавливаются близко друг к другу по всей территории компании. Хотя точки доступа становятся дешевле, общая цена развертывания подобной архитектуры все еще высока.

Реализовать такое плотное развертывание может помочь приложение AirMagnet Survey, являющееся частью семейства анализаторов AirMagnet Wi-Fi Analyzer. С помощью приложения AirMagnet Survey можно:

- Обеспечить надлежащее общее покрытие сигнала.
- Определить идеальное размещение точки доступа и параметры питания.
- Провести количественный анализ источников радиопомех и шумов.
- Определить зоны роуминга клиентов.
- Эмулировать клиентский опыт для измерения реальной скорости соединения, количества повторных попыток и потерь пакетов.
- Обеспечить адекватную полосу пропускания и скорость для любой сети WLAN.



Приложение AirMagnet Survey

Power-Save DTIM Setting not Optimised for Voice (Настройка DTIM для энергосбережения не оптимизирована для передачи голоса)

Описание сигнала тревоги и возможные причины

Значение DTIM играет важную роль в приложениях VoWLAN. Любая неправильная настройка конфигурации здесь, как в случае более высоких значений DTIM, может привести к прерываниям трафика и недовольству пользователей VoWLAN. Большинство производителей предпочитают более низкое значение, которое обеспечивает удовлетворительные результаты для приложений VoWLAN. Единственным недостатком этого является то, что быстрые отклики DTIM могут оказывать огромное влияние на время автономной работы голосовых телефонов или устройств. Согласно стандарту 802.11 станции могут работать в режиме энергосбережения. В этом режиме станции «спят» в течение определенного периода времени (в зависимости от количества сигналов маяка) и просыпаются, чтобы принимать сигналы маяков и искать свой собственный идентификатор в Traffic Indication Map (карте индикации трафика) каждого маяка. После получения сигнала маяка проснувшиеся станции узнают, есть ли какой-либо трафик, буферизованный для них в точке доступа. После того, как точка доступа передаст DTIM, она передаст буферизованные данные.

Идентификатор элемента	Длина	Счетчик DTIM	Период DTIM	Управление битовым массивом	Частичный виртуальный битовый массив

Информационный элемент карты индикации трафика

Важным параметром здесь является период DTIM, который определяет, насколько часто точка доступа будет передавать буферизованные данные. Это значение напрямую выводится из интервала сигнала маяка. Например, если период сигнала маяка составляет 100 мс, а значение DTIM равно 3, то точка доступа будет передавать буферизованные данные каждые 300 мс. У каждого производителя есть собственное рекомендуемое значение DTIM для своих точек доступа.

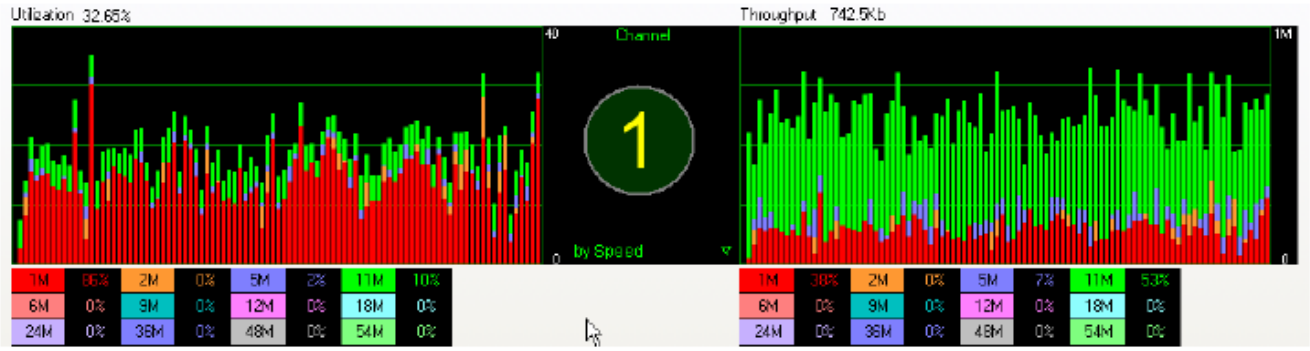
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer предупреждает администратора WLAN, если видит, что значение DTIM отличается от значения, указанного в пороговом значении предупреждения. Пожалуйста, обратитесь к документации используемой точки доступа, чтобы указать нужное значение. Для улучшения функциональности точек доступа при обработке трафика VoWLAN AirMagnet рекомендует проверять наличие собственной реализации (при ее доступности). Некоторые приложения позволяют трафику VoWLAN обходить процесс очереди и быть доступным для немедленной передачи.

Excessive Bandwidth Usage (Чрезмерное использование полосы пропускания)

Описание сигнала тревоги и возможные причины

Спектр WLAN является общедоступной средой с ограничением полосы пропускания. Чтобы обеспечить достаточную доступность сети WLAN, будь то сеть 802.11b со скоростью передачи 11 Мбит/с или 802.11a/g со скоростью передачи 54 Мбит/с, использование полосы пропускания всеми клиентскими устройствами должно тщательно контролироваться для каждого канала и каждого устройства. Имейте в виду, что высокое использование полосы пропускания не означает высокую пропускную способность сети WLAN. Приведенный ниже образец экрана Channel (Канал) приложения AirMagnet Wi-Fi Analyzer показывает использование 32%, но пропускную способность менее 1 Мбит/с. Проблема заключается в низкой скорости передачи, что также графически показано ниже на диаграмме использования для трафика 1 Мбит/с. Проблема может быть связана с тем, что авторизованный пользователь загружает музыку или фильмы из Интернета, что снижает пропускную способность корпоративной сети.



Анализатор WiFi отслеживает использование полосы пропускания WLAN для каждого канала и устройства.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает использование полосы пропускания для каждого канала и беспроводного устройства. Выполняемый приложением AirMagnet WiFi Analyzer расчет полосы пропускания включает заголовок PLCP (Physical Layer Convergence Procedure - процедура сближения физического уровня), преамбулу и фактическую полезную нагрузку кадра. Из-за протокола предотвращения коллизий CSMA практически невозможно даже приблизиться к использованию в 100%. Использование от шестидесяти до семидесяти процентов следует считать чрезвычайно высоким и требующим лучшего обеспечения оборудованием или повышения эффективности, например, только высокоскоростной передачи. При превышении установленного пользователем порога (в процентах использования) приложение AirMagnet Wi-Fi Analyzer подает этот сигнал тревоги. Примите соответствующие меры для устранения этой проблемы. Эти меры могут включать поиск пользователей, которые способны вызывать проблему из-за чрезмерной загрузки файлов из Интернета.

VoWLAN Multicast Traffic Detected (Обнаружен многоадресный трафик VoWLAN)

Описание сигнала тревоги и возможные причины

Точка доступа 802.11 должна немедленно передавать любые многоадресные/широковещательные кадры, если не обнаружены мобильные станции в режиме PSP (Power Save Polling – энергосбережение при опросе). В корпоративной среде часто может присутствовать, по крайней мере, один клиент в режиме энергосбережения. В таких ситуациях кадры будут помещены в очередь и переданы с интервалом между кадрами DTIM (Сообщение с индикацией трафика доставки). Этот интервал может различаться (в зависимости от производителя точки доступа) на 1 - 2 секунды. Следовательно, многоадресный трафик VoWLAN будет доставляться по истечении периода DTIM, что может привести к прерываниям во время голосовых вызовов. Кроме того, когда устройство связано с точкой доступа, многоадресный трафик доставляется с более низкими скоростями передачи данных, что может привести к снижению производительности беспроводной сети LAN.

Существует два способа решения этой проблемы:

- Уменьшение значения DTIM: Большинство продуктов позволяют пользователю устанавливать очень низкое значение. Хотя это простое решение, быстрые ответы DTIM могут оказать огромное влияние на время автономной работы голосовых телефонов или устройств.
- Проприетарные решения: Проприетарные (фирменные) решения могут быть реализованы на уровне точки доступа. Некоторые точки доступа позволяют пользователям для идентификации голосового кадра указывать MAC-адрес многоадресной рассылки. После распознавания точка доступа позволит кадрам обойти процесс постановки в очередь и сделает их доступными для немедленной передачи. Другие, не обозначенные пользователем, кадры многоадресной/широковещательной передачи будут обрабатываться с помощью обычных процедур DTIM. Это решение обеспечивает хороший баланс между удовлетворительным качеством передачи голоса и временем автономной работы. Единственный недостаток заключается в том, что это проприетарные решения, поэтому они будут доступны только на определенных устройствах.

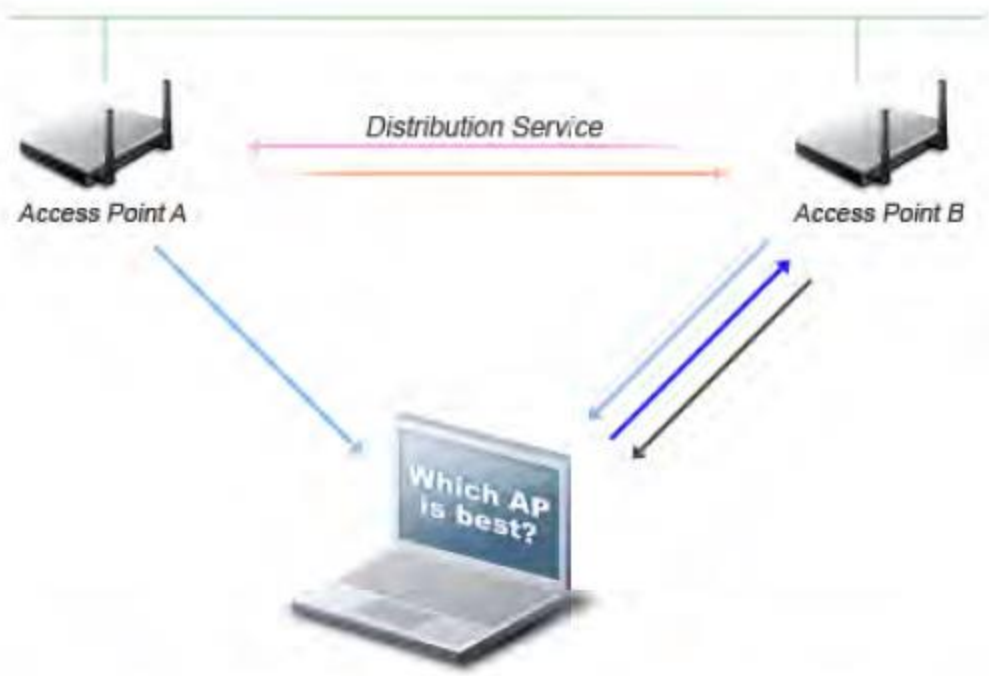
Решение AirMagnet

Приложение AirMagnet W-Fi Analyzer обнаруживает точки доступа, передающие многоадресный трафик. Рекомендуется избегать использования многоадресного трафика для голосовых приложений, таких как Music on Hold (MoH: система Music on Hold воспроизводит предварительно записанную программу, которую абоненты могут слушать, пока они находятся в режиме ожидания; система воспроизводит музыку, голосовое сообщение или комбинацию обоих). Пользователь может выбрать одно из двух решений, упомянутых выше: а) уменьшить значение DTIM или б) использовать проприетарные решения (при их наличии).

Excessive Roaming Detected on Wireless Phones (Обнаружен чрезмерный роуминг беспроводных телефонов)

Описание сигнала тревоги и возможные причины

После успешного подключения к точке доступа клиентские устройства VoWLAN начинают использовать беспроводное соединение для связи, но при этом продолжают поиск лучших беспроводных услуг (например, другую точку доступа с более сильным сигналом, меньшими шумами канала или более высокой поддерживаемой скоростью).



Distribution Service	Услуга распределения
Access Point A (B)	Точка доступа A (B)
Which AP is best?	Какая точка доступа лучше?
1. Адаптер в настоящий момент связан с точкой доступа A, но прослушивает сигналы маяка от всех точек доступа. 2. Адаптер оценивает сигналы маяка точек доступа, выбирая лучший из них. 3. Адаптер передает запрос на подключение на выбранную точку доступа (B). 4. Точка доступа B подтверждает подключение и регистрирует адаптер. 5. Точка доступа B информирует точку доступа A о переподключении на точку доступа B с помощью DS. 6. Точка доступа A передает буферизированные пакеты на точку доступа B и отменяет регистрацию адаптера.	

Устройство VoWLAN переключается на лучшую точку доступа для обеспечения качественной связи

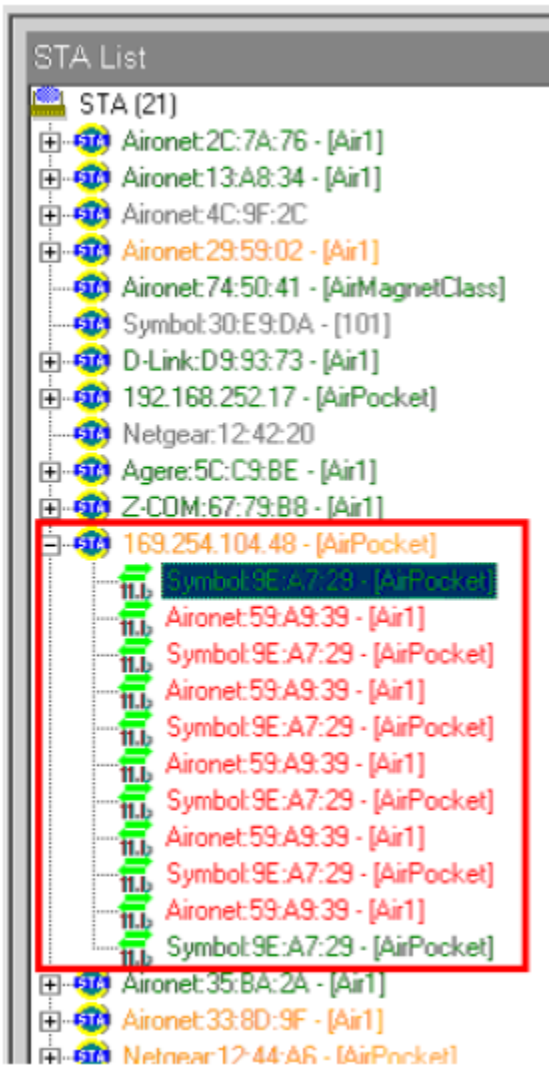
Как только определена точка доступа с лучшим обслуживанием, клиентская станция подключится к ней и разорвет соединение с исходной точкой доступа. Мобильные устройства (телефоны VoWLAN и сканеры штрих-кода) в роуминге в сети WLAN часто выполняют такое повторное подключение. Когда телефоны переключаются от одной точки доступа к другой, вызовы могут быть сброшены, и телефонам может потребоваться выполнить новое зондирование, провести повторное подключение и повторную аутентификацию. Когда устройства VoWLAN выходят из зоны действия одной точки доступа в зону действия другой, задержка передачи обслуживания может составлять от 400 до 600 мс. Это значительная задержка, которая неприемлема для передачи голоса и приведет к разрыву соединения, что будет очень неприятно для пользователей телефонов VoWLAN. Кроме того, существующие стандарты безопасности мало помогают в случае быстрого роуминга; новая рабочая группа 802.11r все еще продолжает вести разработки для улучшения роуминга VoWLAN. Их цель - сократить время, необходимое для аутентификации в роуминге, что позволит лучше поддерживать приложения, работающие в реальном времени, например, голосовые. Благодаря более совершенным технологиям управления WLAN (как те, что перечислены ниже) клиентские станции все менее склонны изменять подключение, чтобы приспособиться к динамической радиочастотной среде:

- Балансировка нагрузки точки доступа и распределение полосы пропускания.
- Динамический выбор канала для предотвращения радиопомех и выделенная полоса пропускания канала.
- Автоматическая регулировка выходной мощности точки доступа для оптимизации покрытия и емкости.

Все эти технологии повышают эффективность сети WLAN. Однако реализации и точная настройка, которые выполняются производителем оборудования, не соответствуют друг другу. Новые незрелые продукты могут приводить к частому повторному подключению сбитых с толку клиентских станций, что приведет к нарушению обслуживания.

Решение AirMagnet

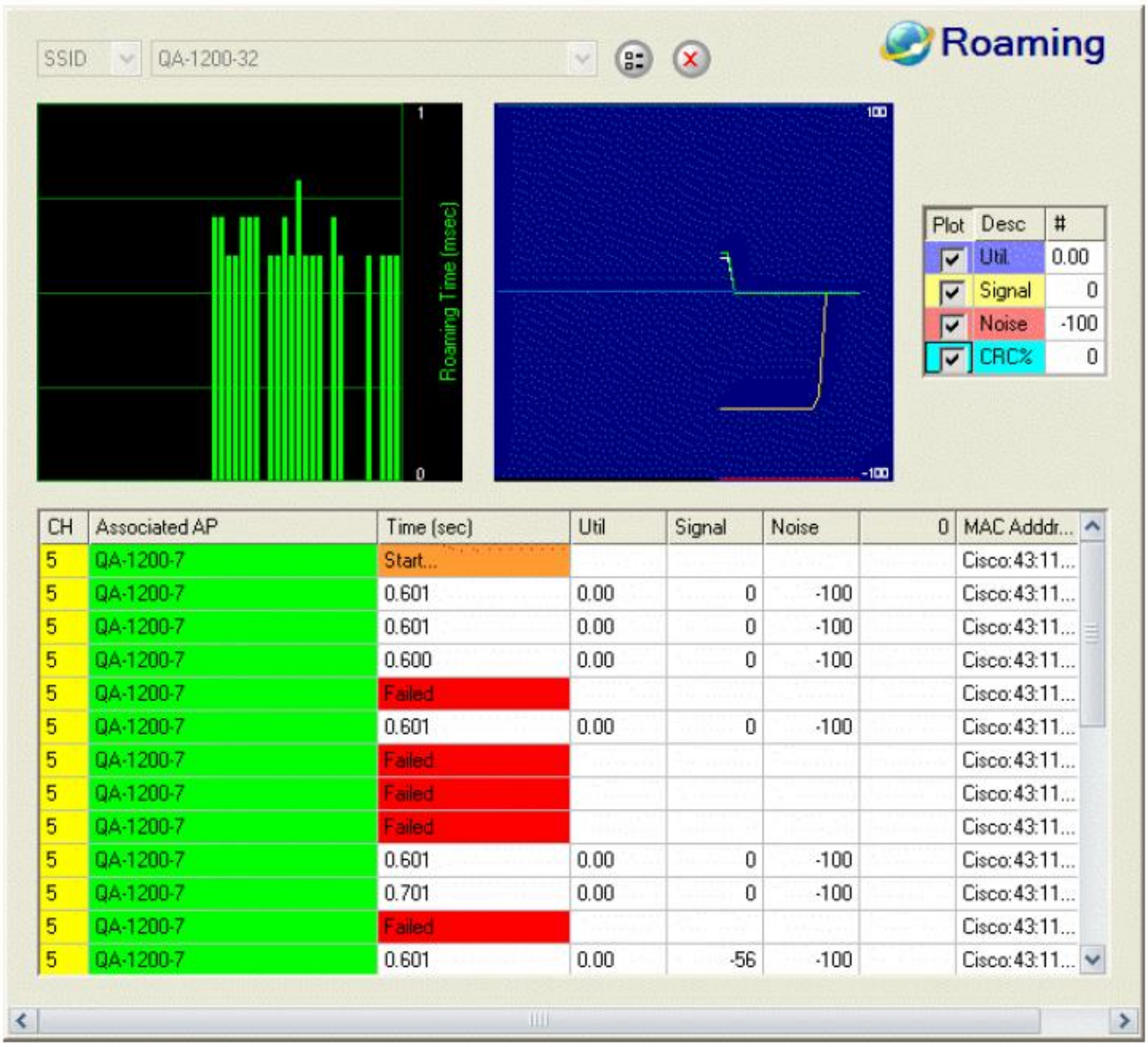
Не ожидается, что стационарные устройства (например, беспроводные принтеры и беспроводные настольные компьютеры) будут склонны к частым повторным подключениям. Приложение AirMagnet WiFi Analyzer отслеживает чрезмерное количество повторных подключений VoWLAN, подсчитывая количество соединений и точек доступа. После обнаружения и получения сообщения от приложения AirMagnet WiFi Analyzer эту проблему можно дополнительно исследовать с помощью списка станций, отображая задействованные точки доступа и характеристики сеанса (смотрите пример ниже).



Станция 169.254.104.48 переключалась между двумя точками доступа 11 раз.

Использование списка станций на странице инфраструктуры (Infrastructure) для исследования проблемы чрезмерного роуминга

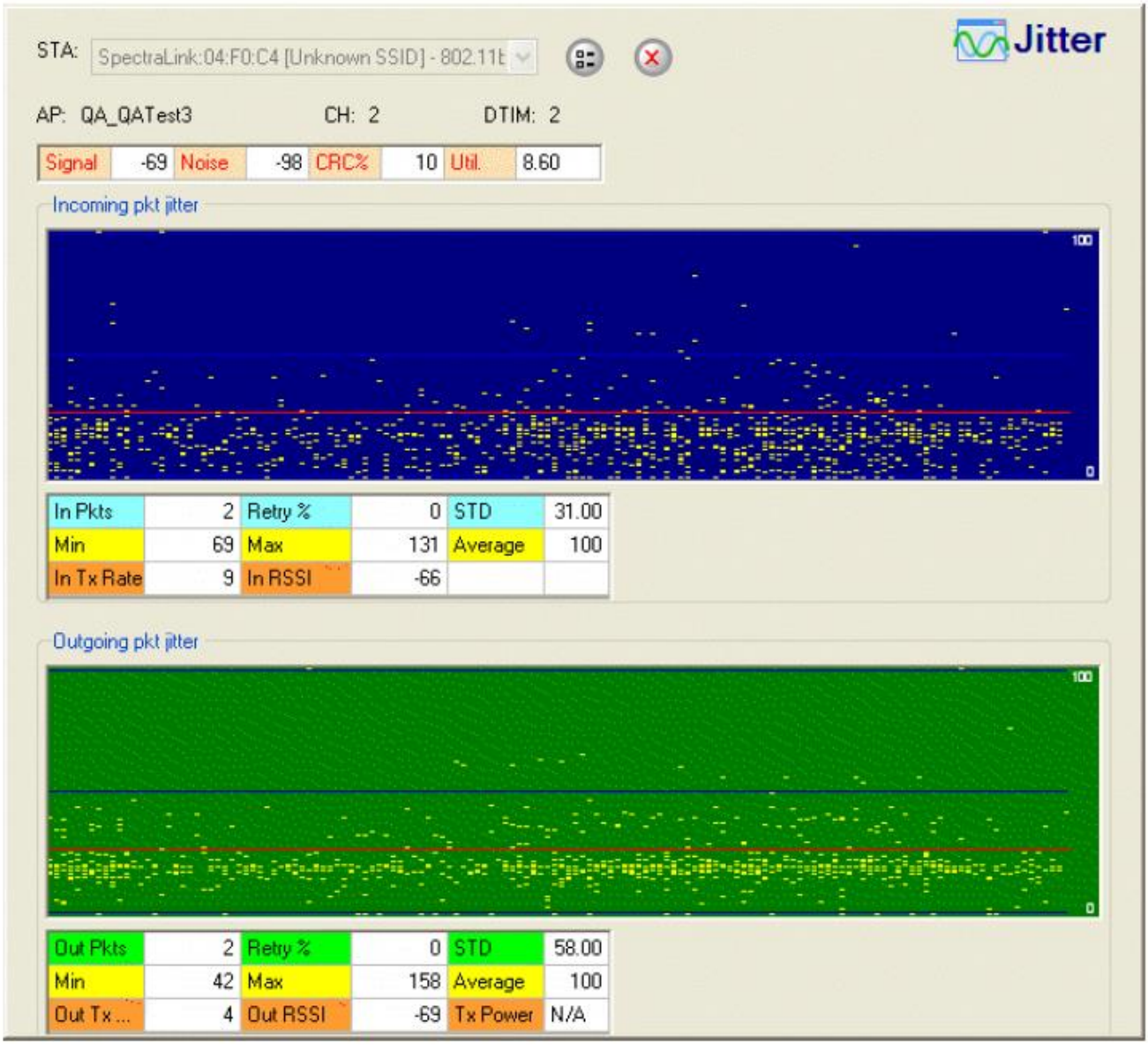
Для измерения задержки роуминга, когда станция отсоединяется от одной точки доступа, а затем пытается установить связь с другой точкой доступа, разработан инструмент AirMagnet Roaming.



CH	Associated AP	Time (sec)	Util	Signal	Noise	0	MAC Adddr...
5	QA-1200-7	Start...					Cisco:43:11...
5	QA-1200-7	0.601	0.00	0	-100		Cisco:43:11...
5	QA-1200-7	0.601	0.00	0	-100		Cisco:43:11...
5	QA-1200-7	0.600	0.00	0	-100		Cisco:43:11...
5	QA-1200-7	Failed					Cisco:43:11...
5	QA-1200-7	0.601	0.00	0	-100		Cisco:43:11...
5	QA-1200-7	Failed					Cisco:43:11...
5	QA-1200-7	Failed					Cisco:43:11...
5	QA-1200-7	Failed					Cisco:43:11...
5	QA-1200-7	0.601	0.00	0	-100		Cisco:43:11...
5	QA-1200-7	0.701	0.00	0	-100		Cisco:43:11...
5	QA-1200-7	Failed					Cisco:43:11...
5	QA-1200-7	0.601	0.00	-56	-100		Cisco:43:11...

Инструмент AirMagnet Roaming, предназначенный для измерения задержек в роуминге

Кроме того, инструмент AirMagnet Jitter позволяет пользователю эффективно измерять джиттер радиочастотного сигнала как во входящем, так и в исходящем трафике WLAN между точкой доступа и станцией. На основе этой информации пользователь для уменьшения помех может внести соответствующие изменения в конфигурацию или размещение точек доступа.

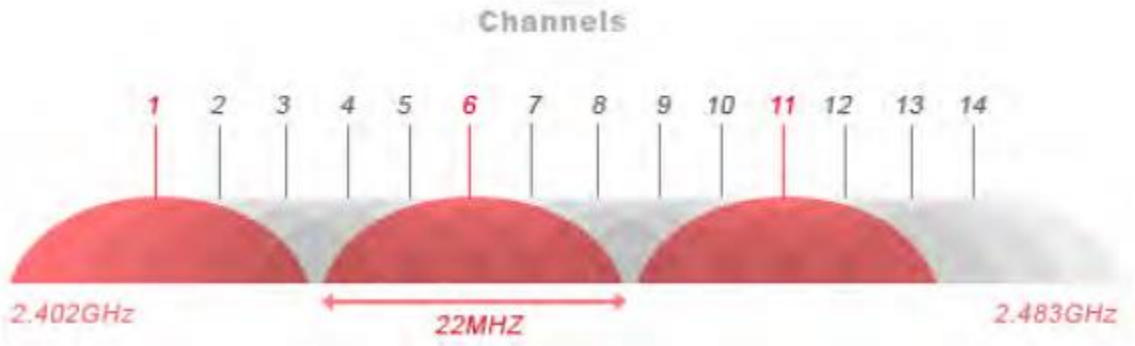


Инструмент AirMagnet Jitter для измерения джиттера

Voice Quality Degradation Caused by Interfering APs (Ухудшение качества голоса, вызванное помехами от точек доступа)

Описание сигнала тревоги и возможные причины

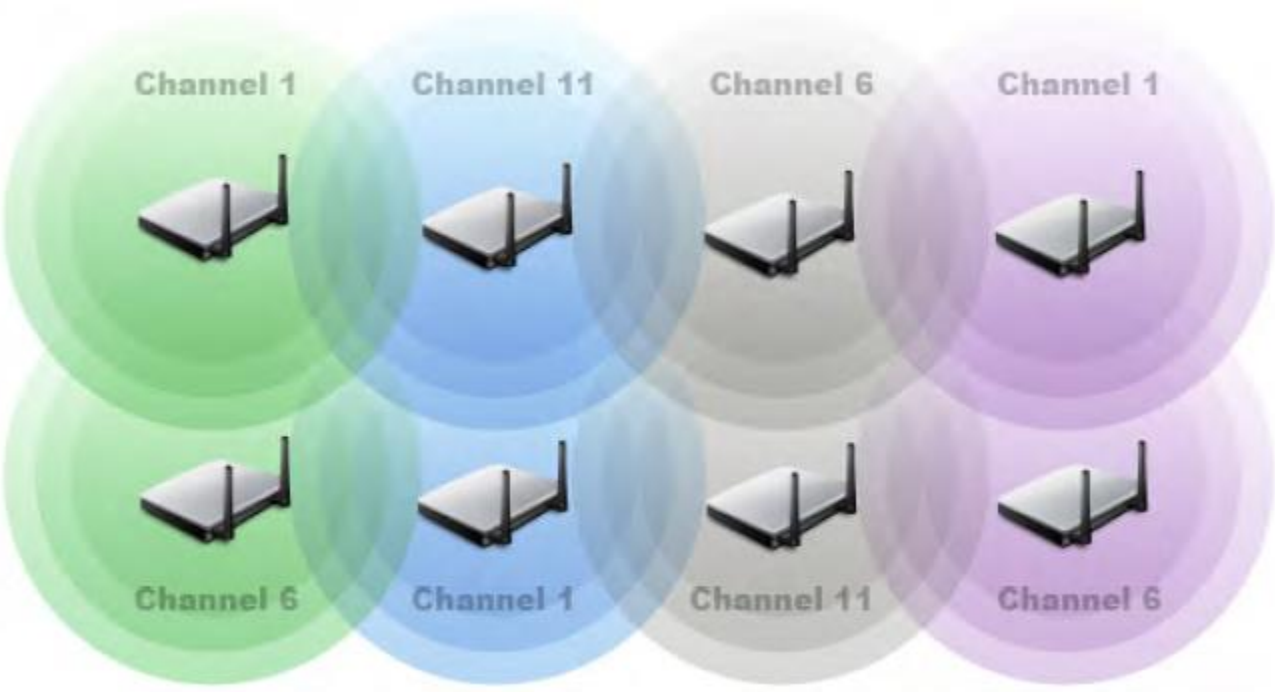
Устройства 802.11b и 11g работают в радиочастотном диапазоне 2,4 ГГц. В этом диапазоне частот стандарт IEEE задает в общей сложности 14 каналов, каждый из которых занимает 22 МГц. Соседние каналы перекрываются друг с другом в радиочастотном спектре (смотрите рисунок ниже).



Channels	Каналы
2.402 GHz	2,402 ГГц
22 MHz	22 МГц
2.483 GHz	2,483 ГГц

Распределение каналов и перекрывание частот для 802.11b и 11g

Используемые беспроводными устройствами, работающими в соседних каналах (номера каналов различаются меньше, чем на 5), радиочастотные полосы перекрываются, и они создают помехи друг другу. В идеальном случае для избежания подобных проблем точки доступа должны отстоять друг от друга на 5 каналов. На рисунке ниже приводится пример распределения каналов и развертывания точки доступа.



Channel	Канал

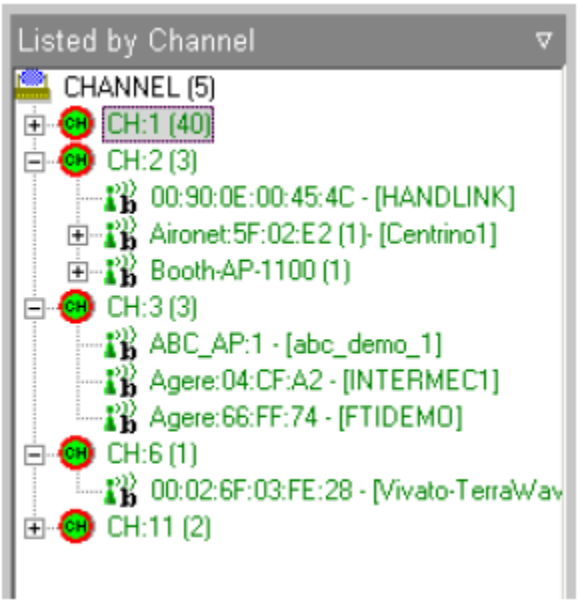
Обследование площадки для выделения неперекрывающихся каналов физически смежным точкам доступа

Помехи этой точки доступа могут быть очень критичными для приложений VoWLAN. Они могут привести к потере пакетов, что вызовет прерывание разговора, и клиенты VoWLAN разорвут свое соединение с точкой доступа, тем самым прервав голосовой вызов. После этого для сохранения возможности совершения голосовых вызовов клиентам может потребоваться повторное подключение и повторная аутентификация. Этот процесс усложняется в среде, где применяются более высокие стандарты безопасности, такие как WPA и 802.11i. Для этого серверного метода аутентификации потребуется дополнительное время на процесс установления связи и получение нового ключа шифрования. Подобное увеличение задержки делает эти механизмы безопасности непривлекательными для приложений

VoWLAN. Более слабые механизмы (такие как WEP), которые поддерживают более быстрые процессы передачи обслуживания, могут проявлять себя немного лучше с точки зрения задержки, джиттера и потери информации.

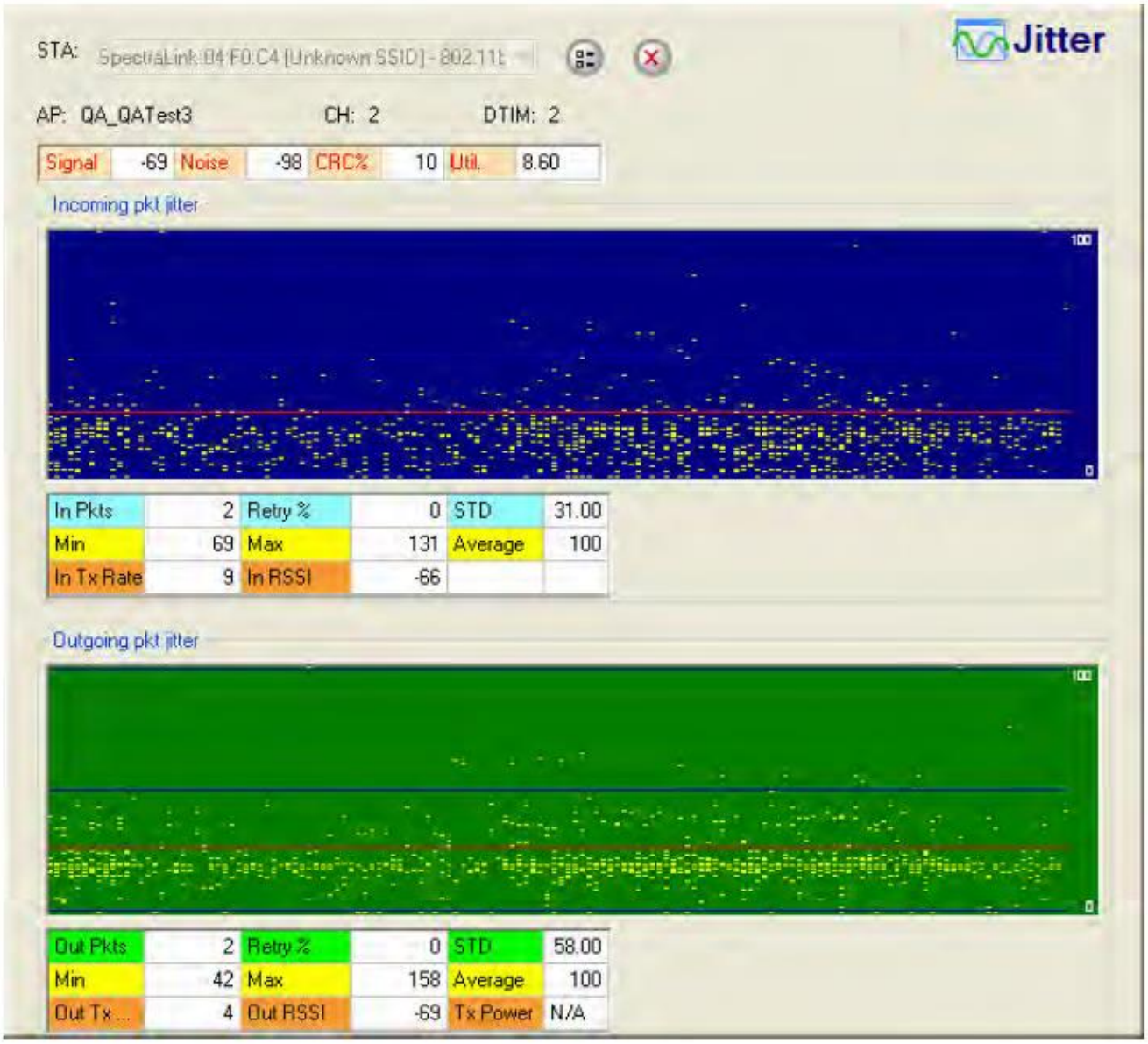
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer анализирует распределение и использование каналов для обнаружения их взаимных помех. Сигнал тревоги подается, когда полоса частот канала перекрывается более чем допустимым числом точек доступа (настраиваемый пользователем порог подачи сигнала тревоги). Например, если приложение AirMagnet WiFi Analyzer обнаруживает 5 точек доступа, работающих в каналах 1, 2, 3, 4, 5 и 6 по отдельности, то сформирует этот сигнал тревоги, чтобы указать, что все эти точки доступа мешают друг другу, а количество точек доступа, использующих перекрывающиеся частоты, превышает пороговое значение по умолчанию, равное 3. Большинство экспертов советуют использовать каналы 1, 6 и 11, а некоторые рекомендуют использовать только каналы 1 и 11. Для дальнейшего изучения текущего использования каналов и выполнения необходимых действий пользователь может использовать экран AirMagnet Infrastructure (показан ниже).



На экране AirMagnet Infrastructure (список по каналам) отображается распределение каналов

Кроме того, инструмент AirMagnet Jitter позволяет пользователю эффективно измерять джиттер радиочастотного сигнала как во входящем, так и в исходящем трафике WLAN между точкой доступа и станцией. На основе этой информации пользователь может внести соответствующие изменения в конфигурацию или размещение точек доступа, чтобы уменьшить помехи.



Инструмент AirMagnet Jitter для измерения джиттера

AP Configuration Changed (Security) (Изменена конфигурация точки доступа (безопасность))

Описание сигнала тревоги и возможные причины

Обычно к точке доступа, работающей без какого-либо механизма шифрования, могут подключаться неавторизованные клиенты без ключей шифрования, которые получат доступ к проводной сети предприятия. Это не только ставит под угрозу конфиденциальность данных пользователя, но и подвергает риску доступ к корпоративной проводной сети. То же самое относится к сетям, в которых используются более слабые механизмы безопасности, например, WEP, или в которых вообще не используются механизмы безопасности.
Внезапные изменения конфигурации безопасности вашей точки доступа могут указывать на то, что неавторизованное лицо получило доступ к точкам доступа и внесло эти изменения (например, заменило более строгие настройки безопасности, такие как WPA2, более слабыми, например WEP, или заменило WPA2-Enterprise на WPA-2 Personal). Эта ситуация может быть очень вредной для конфиденциальности или неприкосновенности частной жизни в сети, поскольку действительные клиенты могут быть заблокированы в сети, а злоумышленники подключаются к ней.

Администратор точки доступа может вносить изменения для повышения безопасности сети (например, переход от более слабых настроек безопасности, таких как WEP, к более сильным, таким как WPA2).

Решение AirMagnet

AirMagnet WiFi Analyzer также предупреждает пользователя о любых внезапных изменениях настроек безопасности точки доступа. Это может означать, что злоумышленник контролирует точку доступа и изменил конфигурацию безопасности. Это способно привести к отключению всех легитимных клиентов от точки доступа, поскольку они теперь не общаются в одной сети.

Подключитесь к точке доступа, конфигурация которой изменилась, назначьте более надежный пароль для входа в точку доступа, верните исходные настройки безопасности и примите строгие меры для предотвращения подобных ситуаций в будущем.
Также, если настройки безопасности были изменены сетевым администратором намеренно для повышения безопасности, пожалуйста, примите соответствующие меры, проинформировав пользователей о повторной настройке параметров их сетевой безопасности на основе корпоративной политики беспроводной сети.

Excessive Missed AP Beacons (Чрезмерное количество пропущенных сигналов маяка точек доступа)

Описание сигнала тревоги и возможные причины

Точки доступа сети WLAN передают кадры маяков с фиксированной скоростью (обычно 10 сигналов маяка в секунду) для уведомления о своих параметрах обслуживания и конфигурации. Беспроводные клиенты используют эти кадры маяка, чтобы узнать о доступных услугах WLAN и их характеристиках для принятия важных решений относительно подключения и роуминга. Кадр маяка включает информацию о SSID, поддерживаемых скоростях, картах индикации трафика, дополнительных параметрах IBSS, информации о синхронизации и т.д.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает кадры маяка для мониторинга качества обслуживания WLAN. Этот конкретный сигнал тревоги отслеживает частоту поступления сигналов маяка от точки доступа для сравнения с объявленной фиксированной частотой для точки доступа. Пропущенные сигналы маяка указывают на ошибки приема, которые могут быть вызваны помехами, многолучевым распространением, шумами, коллизиями и т.п. Чрезмерное количество пропущенных сигналов маяка требует тщательного расследования, так как это может указывать на чрезмерные помехи в сети. Чтобы определить, вызваны ли помехи другим трафиком 802.11, и узнать, какие устройства могут быть причиной проблемы, можно использовать страницу RF Interference (Радиочастотные помехи) приложения AirMagnet WiFi Analyzer.

Non-802.11 Interfering Source Detected (Обнаружен источник помех, отличный от 802.11)

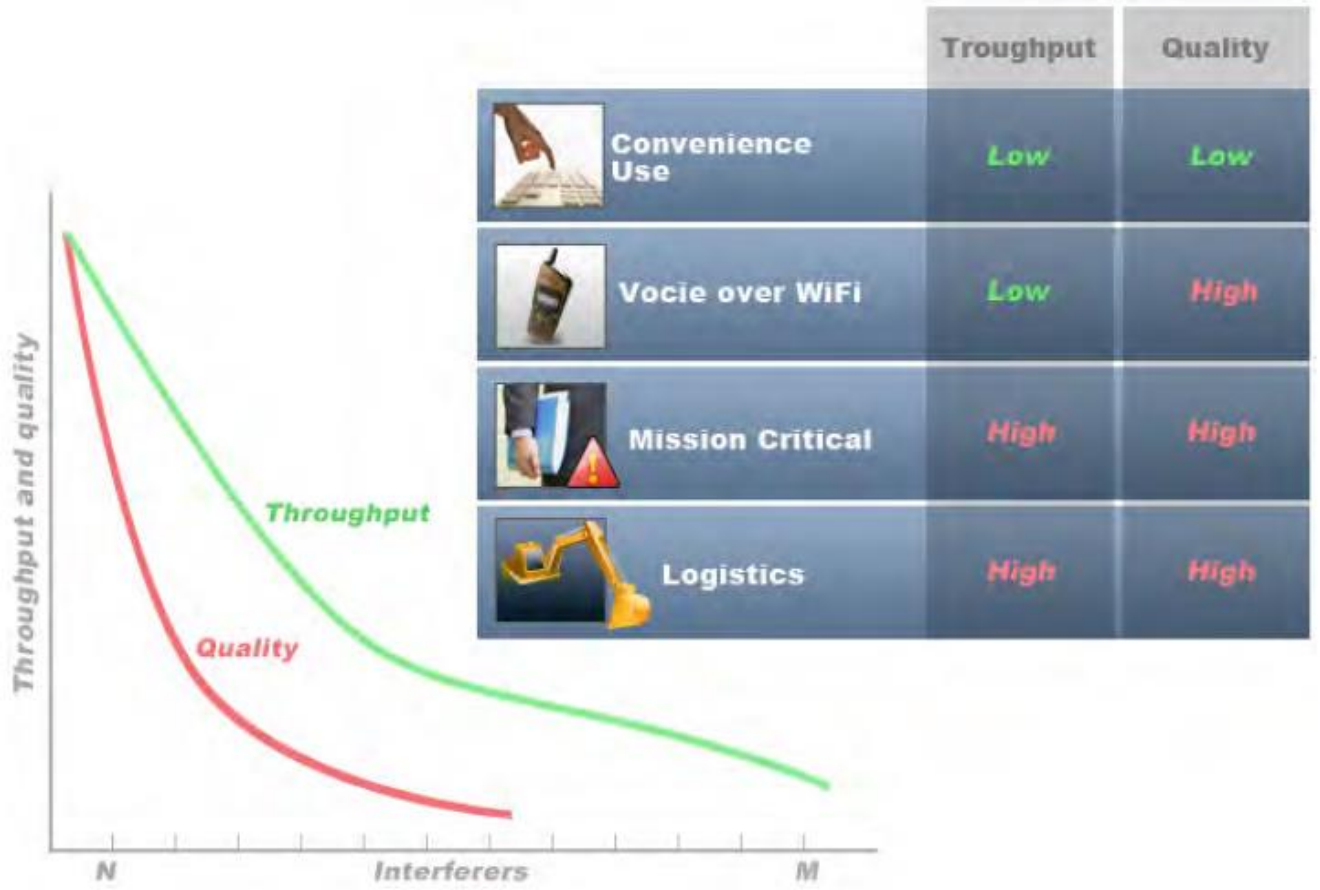
Описание сигнала тревоги и возможные причины

Поскольку сети WLAN работают в нерегулируемых частотных диапазонах 2,4 и 5 ГГц, они подвержены помехам от всех устройств, работающих в этом же частотном спектре. К ним относятся, помимо прочего, микроволновые печи, беспроводные телефоны и гарнитуры, беспроводные камеры систем видеонаблюдения, устройства открывания гаражных ворот, устройства Bluetooth и другие устройства. Также могут существовать помехи в совмещенном и/или соседнем канале, вызванные точками доступа и станциями из соседних сетей WLAN. Чрезмерные радиочастотные помехи могут ухудшить производительность сети 802.11, что приведет к неприемлемо низкой скорости передачи данных и чрезмерной повторной передаче пакетов. Поскольку современные технологии WLAN способны обнаруживать в сети только такие устройства 802.11, как точки доступа и станции, системные администраторы WLAN недостаточно осведомлены о радиочастотной среде, в которой работает их оборудование. У них нет возможности обнаружить источники, не относящиеся к стандарту 802.11, излучающие радиочастотные помехи в нелицензированных диапазонах и способные вызвать нарушение сетевых соединений и многие другие проблемы. Недостаточная осведомленность обо всем радиочастотном спектре не позволяет администраторам сети применять соответствующие меры для повышения производительности своих сетей WLAN перед лицом источников помех и конкурирующих сетей.

Устройства Bluetooth	Микроволновые печи	Беспроводная передача видеосигнала	Радар
Радиорелейные линии	802.11 FH	Сети WiFi	Беспроводные телефоны 2.4/5 ГГц
Игровой контроллер	Наушники	Люминесцентные лампы	

Источники помех, не относящиеся к стандарту 802.11

Приложение AirMagnet WiFi Analyzer, интегрированное с приложением AirMagnet Spectrum Analyzer, включает продуманную технологию обнаружения и классификации источников радиочастотной активности. Используя эти данные, сетевые инженеры смогут предпринять различные действия для повышения производительности и надежности сетей WLAN.



Throughput and Quality	Пропускная способность и качество
Throughput	Пропускная способность
Quality	Качество
Interferers	Источники помех

	Пропускная способность	Качество
Обычное использование	Низкая	Низкое
Голос через WiFi	Низкая	Высокое
Ответственное применение	Высокая	Высокое
Логистика	Высокая	Высокое

Производительность и качество относительно помех

Решение AirMagnet

Совместное использование приложений AirMagnet WiFi Analyzer и Spectrum Analyzer дает пользователям AirMagnet возможность получить обзор уровня 1 для всех экранов поиска и устранения неисправностей WLAN. Это позволяет легко увидеть, когда сеть сталкивается с фундаментальной радиочастотной проблемой. Приложение AirMagnet Spectrum Analyzer может автоматически определять наличие таких отличных от 802.11 источников помех, как микроволновые печи, устройства Bluetooth, беспроводные телефоны и т.д. Если определенная часть частотного спектра постоянно используется другими устройствами, AirMagnet рекомендует сетевому инженеру настроить сеть WLAN таким образом, чтобы избежать передачи по этим каналам. И наоборот, намеренно выполняя поиск «чистых» каналов, устройства WLAN могут быть настроены на широковещательную передачу по этим каналам.

Кроме того, экран Interference (Помехи) приложения AirMagnet Wi-Fi Analyzer дает пользователям возможность визуализировать сводную картину помех, влияющих на качество «эфира» Wi-Fi. Помехи Wi-Fi возникают из-за внутриканальных помех или помех от соседних каналов в корпоративной или соседних сетях WLAN, скрытых узлов в среде Wi-Fi или источников за пределами диапазона 802.11. Помехи вызывают ухудшение работы пользователей сети Wi-Fi, что приводит к замедлению работы приложений и снижению производительности пользователей. Индикатор состояния помех (Interference Status Indicator, второй столбец слева, как показано на рисунке ниже) отображает общее состояние помех для каждого

канала Wi-Fi, рассчитанное на основе оценки помех Wi-Fi для устройств, вносящих свой вклад в создание помех, скрытых узлов и устройств, не относящихся к сети Wi-Fi.

Interference

Channel		#Hidden	#Interferers
Media Type: 802.11g			
1	2.88	0	0
2	0.83	0	0
3	1.47	0	0
4	5.66	0	0
5	24.68	0	0
6	14.43	0	0
7	17.81	0	0
8	7.35	0	0
9	3.04	0	0
10	7.45	0	0
11	12.07	0	0
12	2.47	0	0
13	0.66	0	0
14	0.35	0	0

Состояние помех в канале отображается на экране Interference (Помехи) приложения AirMagnet WiFi Analyzer

Понимание состояния помех для всех каналов позволяет пользователям AirMagnet планировать будущие развертывания Wi-Fi или вносить изменения в существующие сети для повышения их производительности.

- Зеленый цвет означает, что помехи на выбранном канале находятся в допустимых пределах и минимально влияют на производительность сети Wi-Fi.
- Желтый цвет означает, что канал испытывает более сильные, чем обычно, помехи, и что следует найти источник помех и предпринять действия для приведения его в допустимые или желательные пределы.
- Красный цвет означает, что помехи на этом канале превышают рекомендуемые пределы и потенциально могут существенно повлиять на производительность беспроводной сети.

Higher Speed Not Supported (Более высокая скорость не поддерживается)

Описание сигнала тревоги и возможные причины

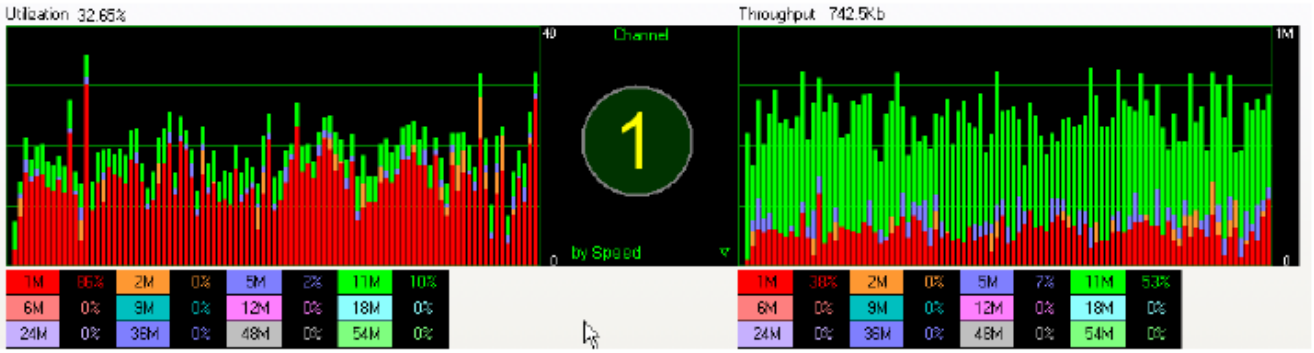
Устройства 802.11a, 11b или 11g от кадра к кадру используют несколько различных скоростей передачи. Более высокая скорость передачи требует меньшей полосы пропускания и обеспечивает более высокую пропускную способность. Оптимизация скорости передачи является ключевым фактором в процессе обследования площадки и развертывания сети WLAN. Обычно скорость зависит от качества сигнала и расстояния. В таблице ниже указаны все поддерживаемые скорости и те значения, которые AirMagnet Enterprise считает высокой скоростью для выбранного стандарта.

Скорость	802.11b (Мбит/с)	802.11g (Мбит/с)	802.11a (Мбит/с)
Поддерживаемая скорость	1, 2, 5.5, 11	1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 54	6, 9, 12, 24, 36, 48, 54

AirMagnet Enterprise считает высокой скоростью	11	54	54

Поддерживаемые скорости и те из них, которые AirMagnet считает «высокой» скоростью

Однако для достижения такого же низкого уровня ошибок, что и при низкоскоростной передаче, высокоскоростная передача требует более высокого качества сигнала. Выбор скорости передачи - это решение, принимаемое передатчиком, который также обнаруживает проблемы приема из-за отсутствия подтверждений. Для повышения надежности передатчик может изменять скорость передачи. Когда это происходит слишком часто, работа сети WLAN замедляется и пропускная способность ухудшается. Обратите внимание на приведенный ниже скриншот экрана приложения AirMagnet WiFi Analyzer. На нем показана чрезмерно низкая скорость передачи (1 Мбит/с), высокая степень использования (32%) и низкая пропускная способность (931 Кбит/с).



Взаимосвязь использования полосы пропускания, пропускной способности и скорости передачи

Решение AirMagnet

Для обеспечения оптимального уровня производительности сети WLAN приложение AirMagnet WiFi Analyzer определяет максимальную поддерживаемую устройством скорость. Если устройство не поддерживает «высокую» скорость передачи (смотрите таблицу выше), приложение AirMagnet WiFi Analyzer выдает этот сигнал тревоги для проведения дальнейшего исследования. Чтобы убедиться, что высокие скорости поддерживаются и включены, проверьте настройки конфигурации точки доступа.

Potential Pre-802.11n Device Detected (Обнаружено потенциальное устройство предварительного стандарта 802.11n)

Описание сигнала тревоги и возможные причины

В январе 2004 года IEEE объявил о создании новой целевой группы 802.11 (TGn) для разработки новой поправки к существующему стандарту для беспроводных локальных сетей. Ожидалось, что эта поправка позволит обеспечить скорость передачи более 100 Мбит/с. Но это предложение прошло долгий путь, и в настоящее время возможны даже более высокие скорости: теоретически они могут достигать значения 540 Мбит/с. Также ожидается, что новый стандарт обеспечит большее рабочее расстояние по сравнению со стандартами 802.11a/g, и будет работать в полосе 2,4 ГГц совместно с устройствами 802.11b/g.

Изначально по стандарту было два предложения:
- WWiSE (World-Wide Spectrum Efficiency) при поддержке таких компаний, как Airgo, Broadcom, Conexant и Texas Instruments, а также
- TGn Sync при поддержке Intel, Atheros, Marvell, Agere и Philips.

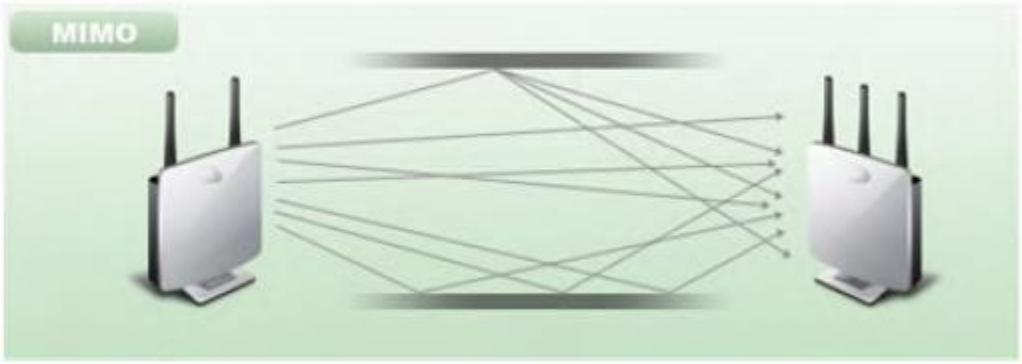
Оба предложения похожи, хотя различаются по своим целям: увеличение пиковых скоростей передачи данных против повышения эффективности. Предложения:

- Позволяют использовать технологию множественного ввода/вывода (MIMO),
- Имеют обратную совместимость с устройствами 802.11b/g,
- Поддерживают работу в текущих каналах 20 МГц и могут использовать каналы двойной ширины 40 МГц для увеличения пропускной способности, а также

- Обеспечивают блоковые подтверждения или пакетную передачу кадров.

Технология MIMO

Несмотря на то, что в стандарте 802.11 использовалось разнесение, для передачи или приема применялась только одна антенна, поскольку для обработки сигнала был доступен только один компонент. Благодаря новой технологии MIMO к каждой антенне для обработки сигналов подключено несколько компонентов (2 или более). Эта технология также использует преимущество многолучевого распространения. Это резко контрастирует с недостатками, на которые жаловались пользователи многопутевого режима. Несколько антенн используются для разделения одного быстрого сигнала на несколько более медленных сигналов. Эти сигналы отправляются через разные антенны и собираются приемником после сортировки ненужных сигналов.

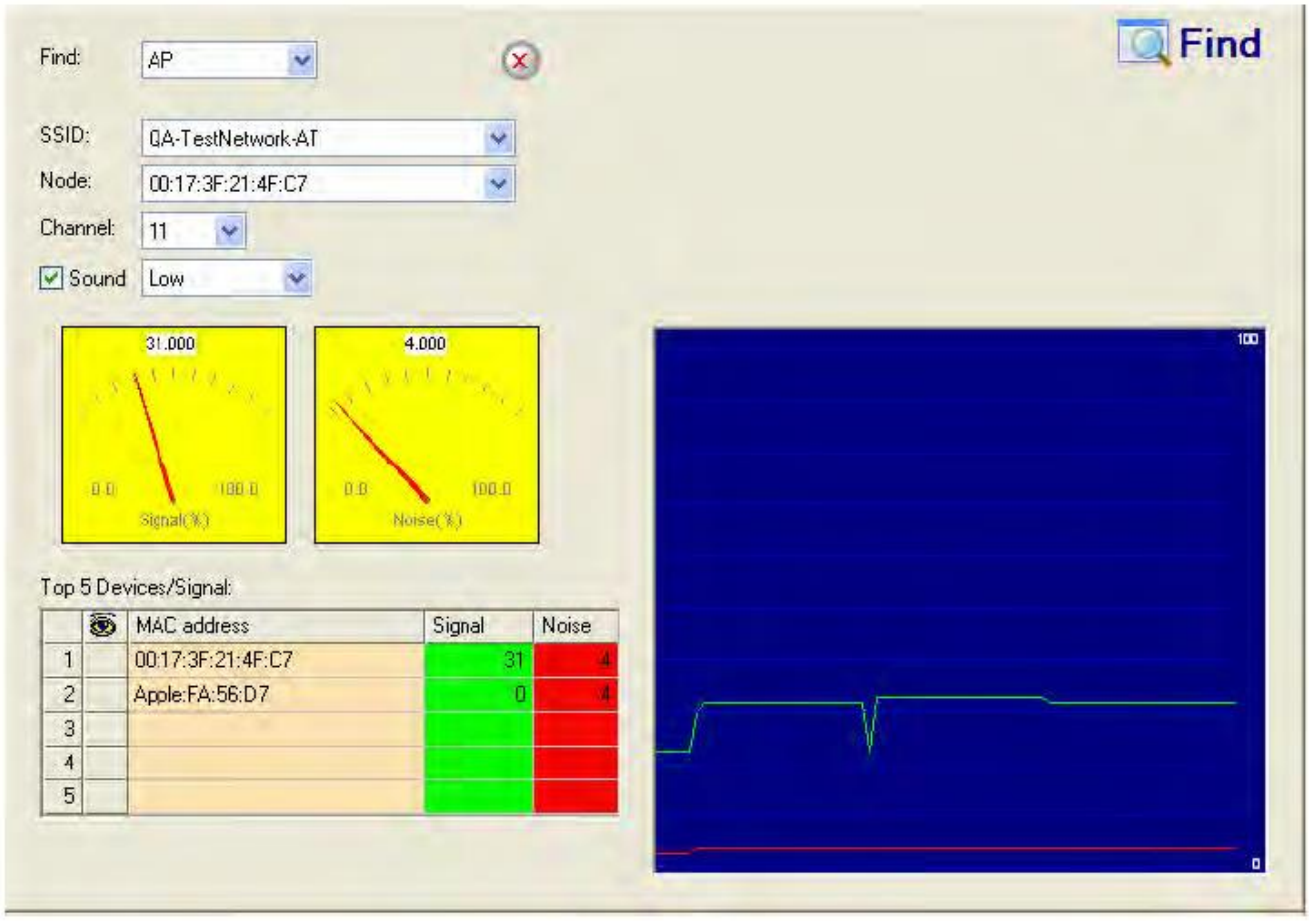


Точки доступа MIMO обмениваются данными между собой

Предложения были объединены, новый проект был подготовлен и представлен на утверждение рабочей группе IEEE 802.11n. Рабочая группа IEEE проголосовала против продвижения этого проекта. Ожидается, что стандарт 802.11n не будет утвержден до июля 2007 года.
Между тем, разные производители разработали свои собственные версии точек доступа «Pre-n». Этот стандарт не является окончательным стандартом 802.11n и, следовательно, может быть несовместим с устройствами, выпущенными после его ратификации. Кроме того, проведенные отраслевыми экспертами первоначальные испытания показали, что, хотя эти устройства и способны обеспечить более высокие скорости на небольших расстояниях, с увеличением расстояния их производительность может быстро снижаться. Некоторые тесты доказали, что если имеющиеся устройства 802.11g работают в каналах, соседних с устройствами pre-n, производительность обоих устройств сильно ухудшается.

Решение AirMagnet

Если приложение AirMagnet WiFi Analyzer обнаруживает устройство Pre-11n в беспроводной среде, оно предупреждает администратора сети WLAN. Присутствие таких устройств может серьезно снижать производительности текущей беспроводной сети из-за проблем взаимодействия между различными стандартами. AirMagnet рекомендует пользователям дождаться ратификации стандарта и внедрения сертификации Wi-Fi. Если эта точка доступа не является известным устройством, используйте инструмент FIND (Найти) для ее поиска.

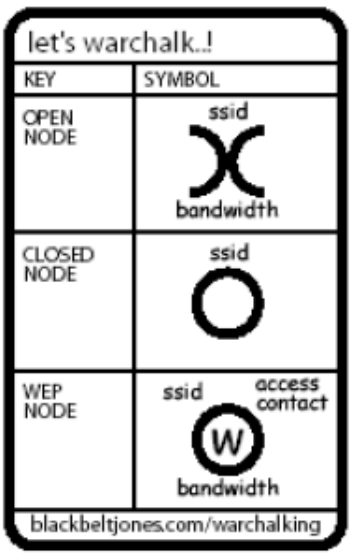


Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

NetStumbler Victim Detected (Обнаружена жертва NetStumbler)

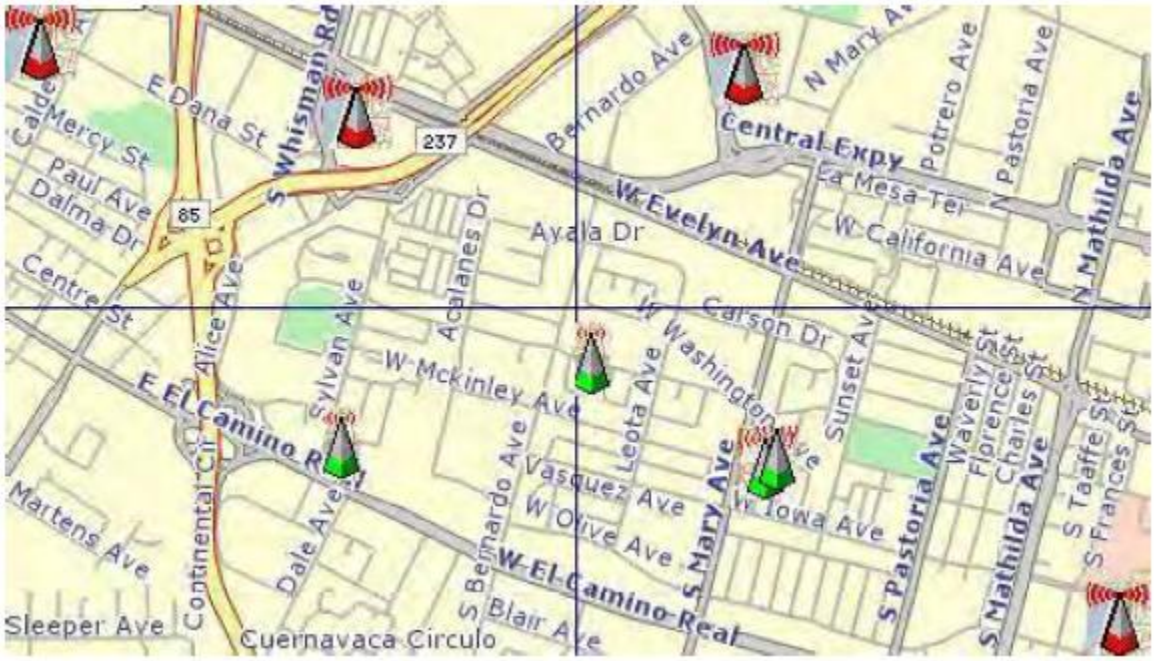
Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer обнаруживает беспроводные клиентские станции, зондирующие сеть WLAN и пытающиеся установить соединение (то есть выдающие запрос соединения с точкой доступа с любым идентификатором SSID) с помощью инструмента NetStumbler. Сигнал тревоги об устройстве, зондирующем точки доступа, выдается, когда хакеры используют более новые версии инструмента NetStumbler. Для более старых версий приложение AirMagnet WiFi Analyzer генерирует сигнал об обнаружении NetStumbler.



С помощью этих универсальных символов нарушитель (war-chalker) обнародует обнаруженную сеть WLAN и ее конфигурацию в районе расположения этой сети.

NetStumbler - это наиболее широко используемый инструмент для ведения обнаружения бесплатных беспроводных сетей с помощью так называемых методов war-driving, war-walking и war-chalking. Хакер беспроводной сети использует инструменты war-driving для обнаружения точек доступа и публикации информации о них (MAC-адреса, SSID, реализованной безопасности и т.д.) в сети Интернет с информацией о географическом местоположении точек доступа. War-chalker'ы обнаруживают точки доступа WLAN и наносят конфигурацию WLAN в общественных местах с помощью показанных выше универсальных символов. War-walking отличается от war-driving тем, что хакер идет пешком, а не едет на машине. Веб-сайт NetStumbler (http://www.netstumbler.com/) предлагает программное обеспечение MiniStumbler для использования на карманных компьютерах, что избавляет злоумышленника от ношения тяжелого ноутбука. Также он поддерживает больше карт, чем Wellenreiter, еще один широко используемый инструмент сканирования. War-walker'ы любят использовать MiniStumbler и аналогичные продукты для обследования торговых центров и крупные розничных магазинов. War-flying - это, как следует из названия, поиск беспроводных сетей с воздуха. Используется то же оборудование, но из низколетящего частного самолета с мощными антеннами. Сообщалось, что такой хакер из города Перт в Австралии во время полета получал сообщения электронной почты и сеансы Internet Relay Chat (ретранслируемого интернет-чата) с высоты 1500 футов (450 метров).

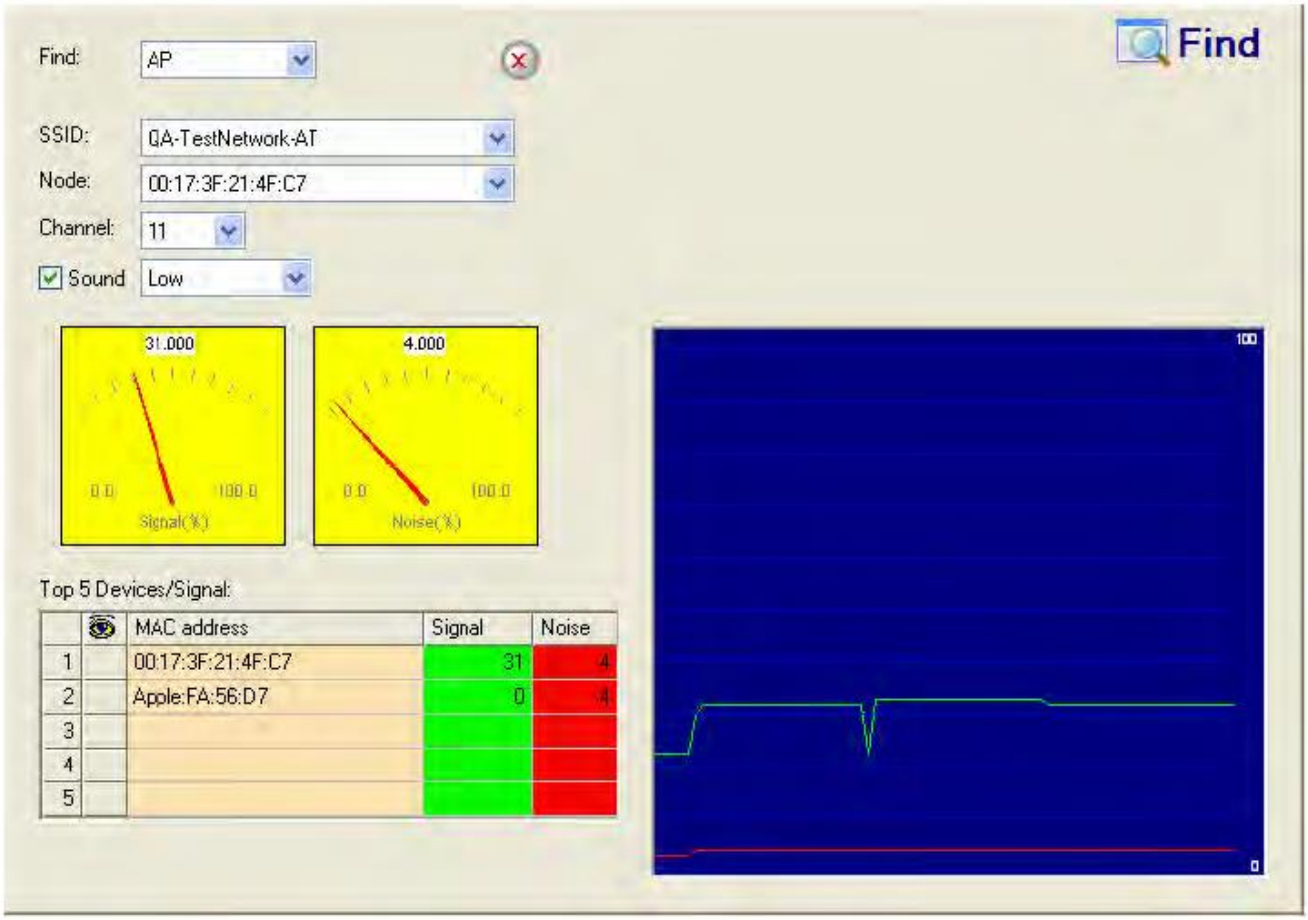


Расположение точек доступа 802.11, опубликованное в Интернете группами war-driving

Приложение AirMagnet WiFi Analyzer предупреждает пользователя, когда обнаруживает станцию с запущенным инструментом Netstumbler, пытающуюся подключиться к корпоративной точке доступа.

Решение AirMagnet

Чтобы предотвратить обнаружение ваших точек доступа подобными средствами взлома, можно настроить точки доступа своей сети так, чтобы они не транслировали свой идентификатор SSID. Можно использовать приложение AirMagnet WiFi Analyzer, чтобы определить, какая из ваших точек доступа транслирует (объявляет) свой идентификатор SSID в сигналах маяка. Кроме того, можно использовать инструмент Find (Найти) в AirMagnet WiFi Analyzer, чтобы физически найти станцию, на которой запущен Netstumbler, или корпоративную точку доступа, с которой эта станция связана. Смотрите рисунок ниже.

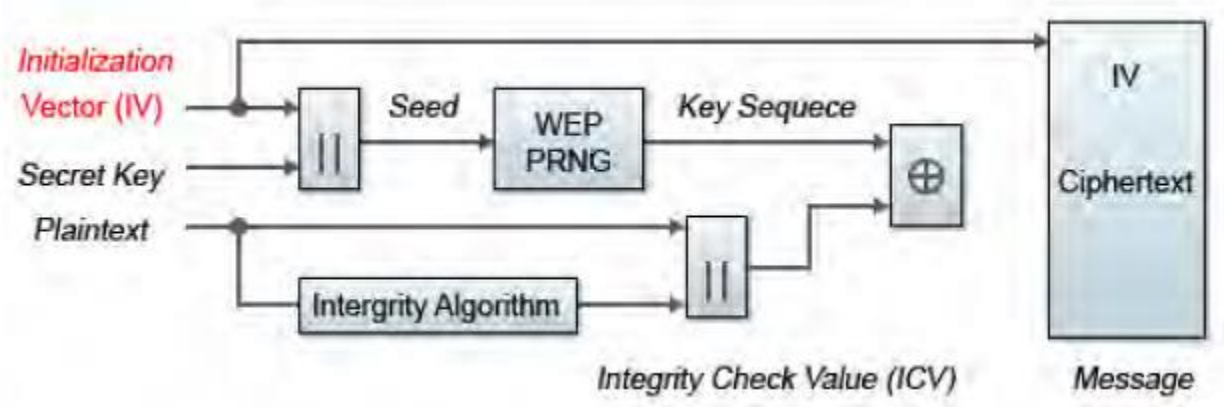


Инструмент Find (Найти) приложения AirMagnet WiFi Analyzer, используемый для отслеживания беспроводных устройств

Potential Chopchop Attack in Progress (Осуществляется потенциальная атака Chopchop)

Описание сигнала тревоги и возможные причины

Хорошо известно, что устройство WLAN, использующее для шифрования статический ключ WEP, уязвимо для различных атак взлома WEP (Обратитесь к документу «Weaknesses in the Key Scheduling Algorithm of RC4 – I» (Слабые стороны алгоритма планирования ключей RC4 – I), авторы Scott Fluhrer, Itsik Mantin и Adi Shamir (Скотт Флурер, Ицик Мантин и Ади Шамир)).



Initialization Vector (IV)	Вектор инициализации (IV)
Seed	Сид
Key Sequence	Последовательность ключа
Secret Key	Секретный ключ
Plaintext	Открытый текст
Integrity Algorithm	Алгоритм целостности
Ciphertext	Зашифрованный текст
Integrity Check Value (ICV)	Значение проверки целостности (ICV)
Message	Сообщение

Блок-схема процесса шифрования WEP

Взлом злоумышленником секретного ключа WEP приводит к отсутствию защиты шифрованием, что ставит под угрозу конфиденциальность данных. Ключ WEP, который в большинстве случаев является 64-битным или 128-битным (некоторые производители также предлагают 152-битное шифрование), состоит из секретного ключа, сконфигурированного пользователем, соединенного с 24-битным IV (вектором инициализации). Инструмент chopchop был написан Korek для операционной системы Linux, чтобы использовать слабые места в WEP и расшифровать пакет данных WEP. Однако инструмент chopchop показывает только открытый текст. На начальном этапе злоумышленник использует файл захвата ранее введенного пакета и расшифровывает пакет, повторно передавая модифицированные пакеты в атакуемую сеть. После завершения атаки инструмент chopchop создаст файл захвата незашифрованных пакетов и другой файл с информацией PRGA (Pseudo Random Generation Algorithm - алгоритм псевдослучайного генерирования), определенной в процессе дешифрования. Затем PGRA подвергается операции XOR с шифротекстом для получения открытого текста.

```
aireplay-ng -4 -h XX:XX:XX:XX:XX:XX -b YY:YY:YY:YY:YY:YY ath0
Where:
•-4 means the chopchop attack
•-h XX:XX:XX:XX:XX:XX is the MAC address of an associated client
or your card's MAC if you did fake authentication
•-b YY:YY:YY:YY:YY:YY is the access point MAC address•ath0 is the
wireless interface name
```

Команды для инициализации атаки Chopchop

Существует несколько точек доступа, которые могут быть неуязвимы для такого рода атак. Они отбрасывают пакеты данных короче 60 байт. Если точка доступа отбрасывает пакеты короче 42 байт, aireplay будет пытаться угадать остальные недостающие данные, поскольку заголовки предсказуемы. Если захватывается IP-пакет, после угадывания его недостающих частей дополнительно проверяется правильность контрольной суммы заголовка. Для этой атаки требуется как минимум один пакет данных WEP. Атака chopchop также работает против динамических конфигураций WEP. Приложение AirMagnet Wi-Fi Analyzer способно обнаруживать потенциальные атаки с использованием инструмента chopchop.

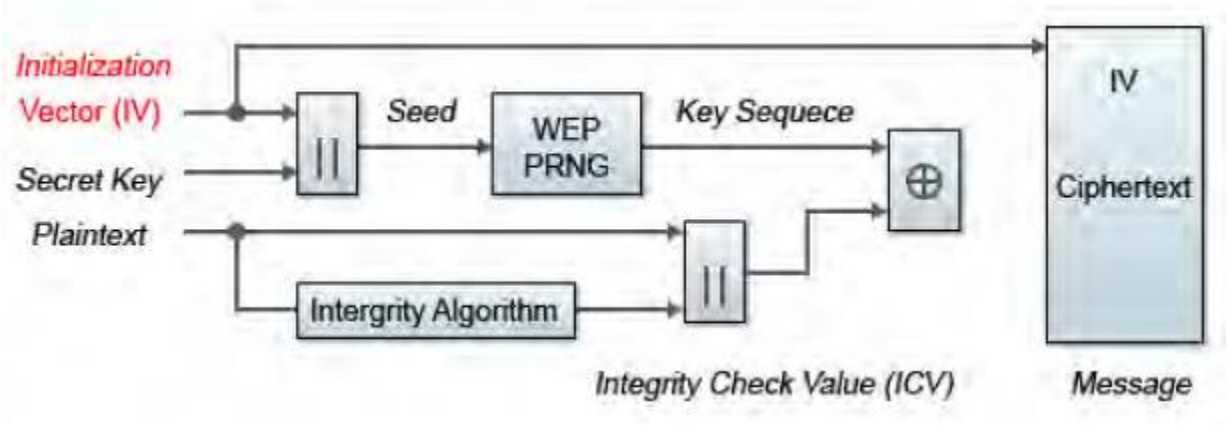
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer предупреждает об обнаружении осуществляемой потенциальной атаки chopchop. AirMagnet рекомендует не использовать WEP в корпоративной среде и принять соответствующие меры, чтобы избежать дыр в сетевой безопасности и обновить инфраструктуру беспроводной сети и устройства до более безопасного стандарта IEEE 802.11i.

Potential Fragmentation Attack in Progress (Осуществляется потенциальная атака фрагментации)

Описание сигнала тревоги и возможные причины

Хорошо известно, что устройство WLAN, использующее для шифрования статический ключ WEP, уязвимо для различных атак взлома WEP (Обратитесь к документу «Weaknesses in the Key Scheduling Algorithm of RC4 – I» (Слабые стороны алгоритма планирования ключей RC4 – I), авторы Scott Fluhrer, Itsik Mantin и Adi Shamir (Скотт Флурер, Ицик Мантин и Ади Шамир)).



Initialization Vector (IV)	Вектор инициализации (IV)
Seed	Сид
Key Sequence	Последовательность ключа
Secret Key	Секретный ключ
Plaintext	Открытый текст
Integrity Algorithm	Алгоритм целостности
Ciphertext	Зашифрованный текст
Integrity Check Value (ICV)	Значение проверки целостности (ICV)
Message	Сообщение

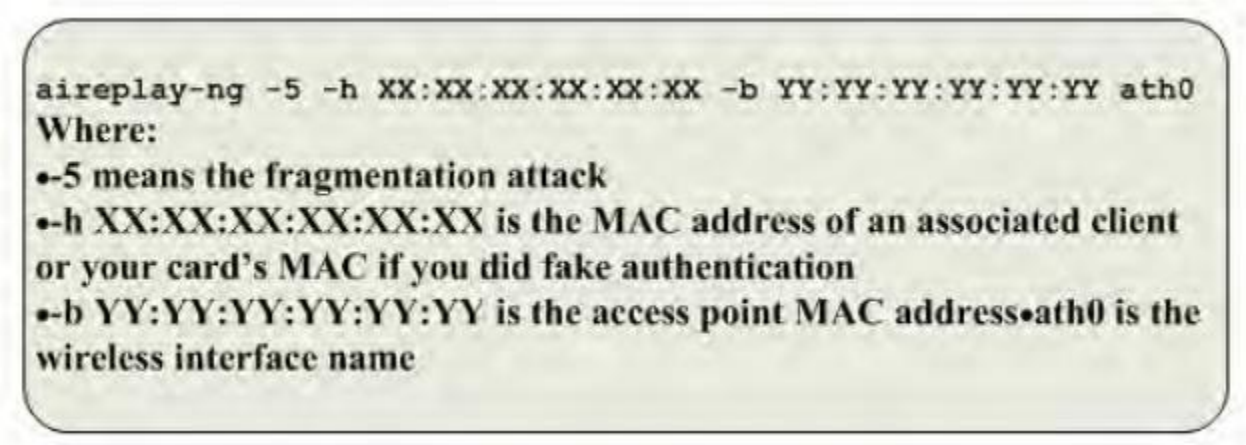
Блок-схема процесса шифрования WEP

Взлом злоумышленником секретного ключа WEP приводит к отсутствию защиты шифрованием, что ставит под угрозу конфиденциальность данных. Ключ WEP, который в большинстве случаев является 64-битным или 128-битным (некоторые производители также предлагают 152-битное шифрование), состоит из секретного ключа, сконфигурированного пользователем, соединенного с 24-битным IV (вектором инициализации).

Согласно http://www.aircrack-ng.org/doku.php?id=fragmentation&s=fragmentation, программа aircrack получает небольшой объем ключевого материала из пакета, а затем пытается отправить пакеты ARP и/или LLC с известной информацией на точку доступа. Если пакет успешно отражен точкой доступа, то из

возвращенного пакета может быть получен больший объем ключевой информации. Этот цикл повторяется несколько раз, пока не будет получено 1500 байтов (в некоторых случаях меньше) PRGA.

Данная атака не восстанавливает сам ключ WEP, а просто получает PRGA. Затем PRGA можно использовать для генерации пакетов с «packetforge-ng», которые применяются для различных атак путем внедрения.



Команды для запуска атаки фрагментации

Приложение AirMagnet WiFi Analyzer обнаруживает потенциальные атаки фрагментации на сеть Wi-Fi.

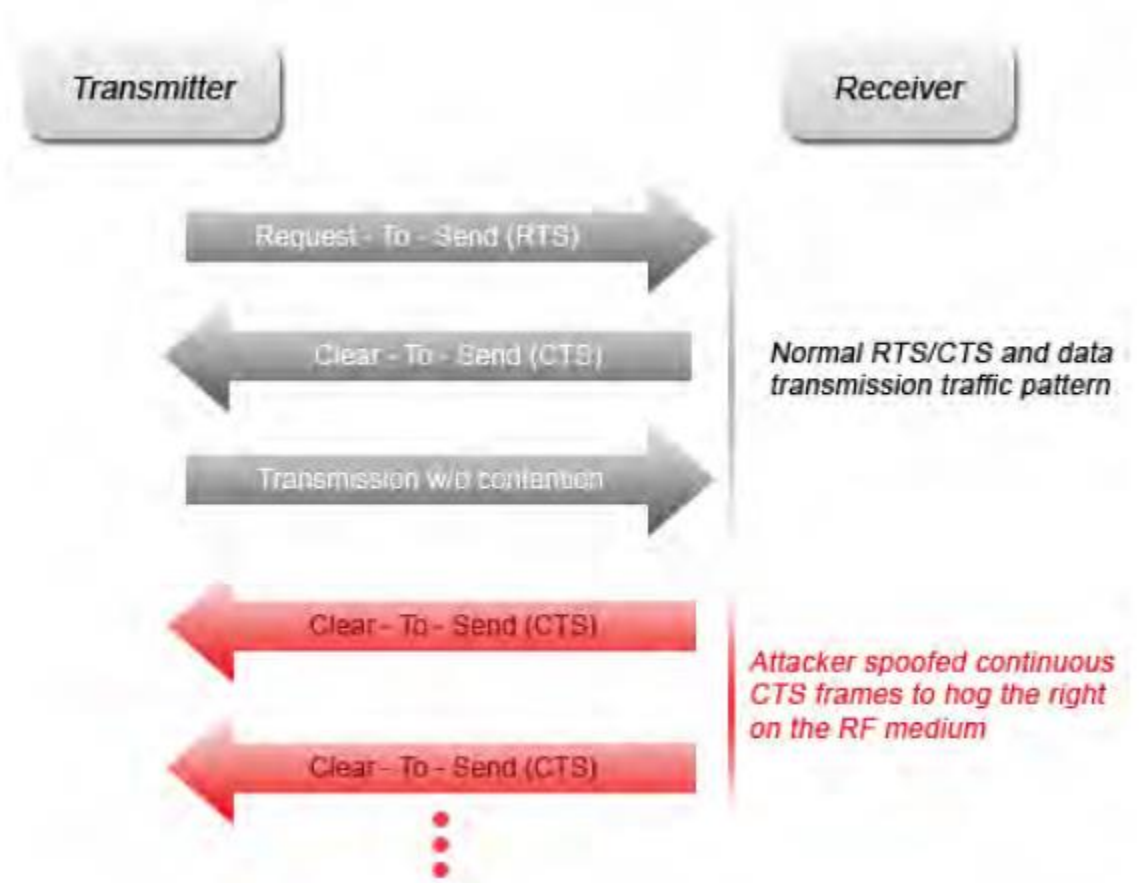
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer предупреждает об обнаружении проведения потенциальной атаки фрагментации. AirMagnet рекомендует не использовать WEP в корпоративной среде и принять соответствующие меры, чтобы избежать дыр в сетевой безопасности и обновить инфраструктуру беспроводной сети и устройства до более безопасного стандарта IEEE 802.11i.

Denial of Service: TRS Flood (Отказ в обслуживании: Флуд RTS)

Описание сигнала тревоги и возможные причины

В качестве дополнительной функции управления доступом станций к радиочастотной среде стандарт IEEE 802.11 использует функцию RTS/CTS (Request-To-Send/Clear-To-Send – готовность к передаче/готовность к приему). Готовое к передаче беспроводное устройство отправляет кадр RTS, чтобы получить на определенный период времени право на использование радиочастотной среды. Приемник предоставляет передатчику право использования радиочастотной среды, отправляя кадр CTS той же длительности. Все беспроводные устройства, обнаружившие кадр CTS, должны предоставить радиочастотную среду передатчику для осуществления передачи без конкуренции. Смотрите рисунок ниже.



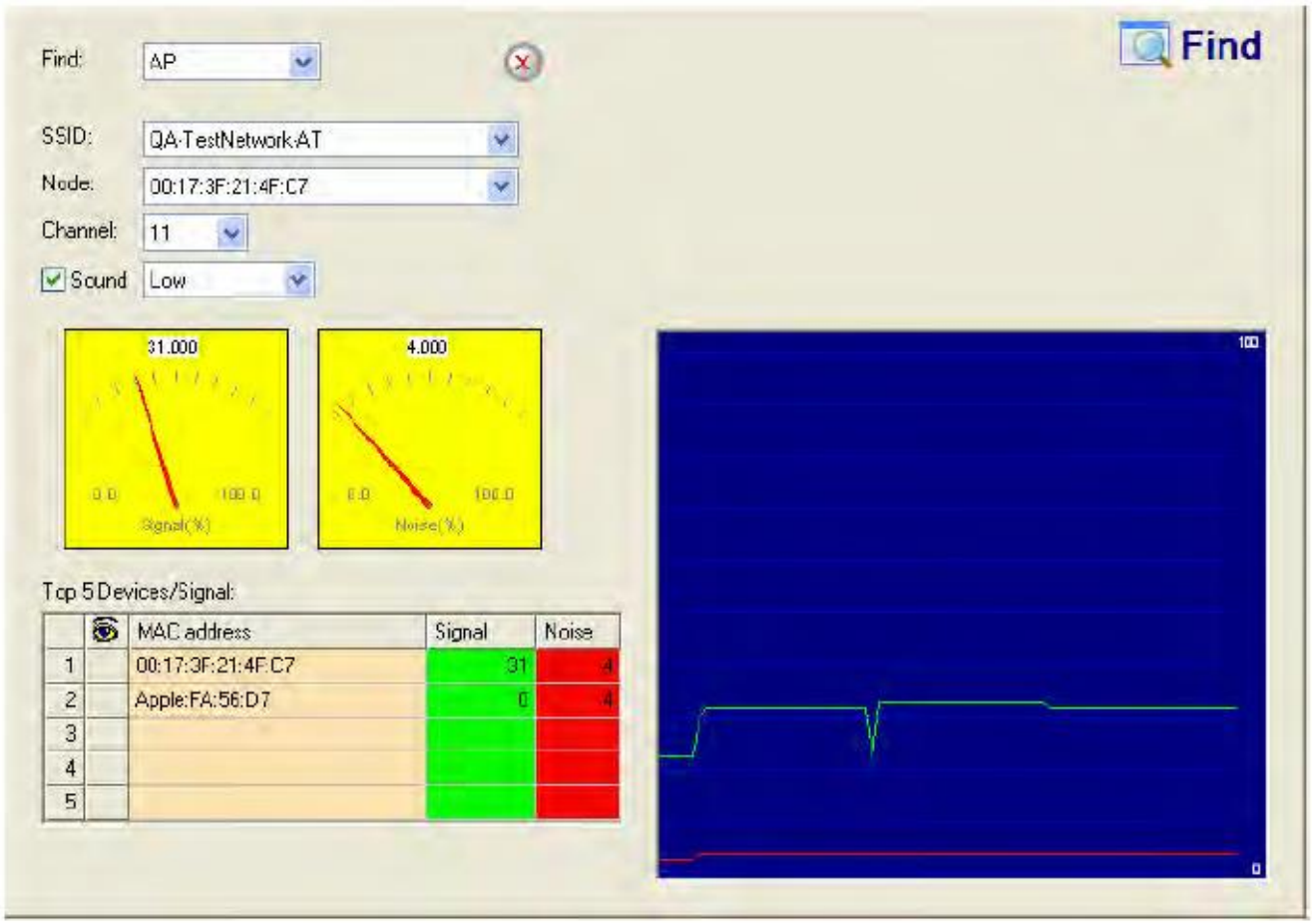
Transmitter	Передатчик
Receiver	Приемник
Request-to-Send (RTS)	Готовность к передаче
Clear-to-Send (CTS)	Готовность к приему
Normal RTS/CTS and data transmission…	Нормальный шаблон передачи трафика для RTS/CTS и данных
Transmission w/o contention	Передача без конкуренции
Attacker spoofed continuous CTS frames…	Атакующий подделывает непрерывный поток кадров CTS для захвата права на радиочастотную среду

Стандартный механизм RTS/CTS и внедренная злоумышленником DoS-атака RTS

Злоумышленник, использующий атаку «отказ в обслуживании» на беспроводную сеть, может воспользоваться привилегией, предоставленной кадру CTS, чтобы зарезервировать радиочастотную среду для передачи. Посредством последовательной передачи кадров RTS с полем большой продолжительности передачи злоумышленник может зарезервировать беспроводную среду и заставить другие беспроводные устройства, совместно ее использующие, сдерживать свои передачи.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает злоупотребление кадрами RTS для проведения DoS-атаки (атаки типа «отказ в обслуживании»). Как и в случае атаки с намеренными радиочастотными помехами, сотрудники службы безопасности могут использовать инструмент FIND (Найти) приложения AirMagnet Wi-Fi Analyzer для определения источника избыточных кадров RTS.



Инструмент Find (Найти) приложения AirMagnet WiFi Analyzer обнаруживает источник атаки RTS-флуд

Device Unprotected by EAP-TTLS (Устройство не защищено EAP-TTLS)

Описание сигнала тревоги и возможные причины

Extensible Authentication Protocol (EAP – Протокол расширенной аутентификации) - это базовая структура безопасности, которая предоставляет средства для улучшения шифрования транзакций 802.11. Данная структура может работать в паре с широким спектром различных механизмов аутентификации, включая версию, известную как Tunneled Transport Layer Security (TTLS – Безопасность на туннельном транспортном уровне). EAP-Tunneled Transport Layer Security (EAP-TTLS) - это протокол EAP, расширяющий TLS (Безопасность транспортного уровня). Протокол EAP-TTLS обеспечивает такую же надежную безопасность, как EAP-TLS, но не требует выдачи сертификатов клиентам. Аутентификация пользователя по-прежнему выполняется с помощью паролей, но учетные данные туннелируются.

Устройства, настроенные для использования протокола EAP, но не механизма аутентификации TTLS, могут представлять собой потенциально небезопасные подключения к беспроводной сети. Хотя такие механизмы облегчают и ускоряют подключение конечных пользователей, в результате получить доступ к критически важным корпоративным данным могут также злоумышленники. Злоумышленникам может быть проще перехватить и декодировать обмен EAP, не защищенный аутентификацией TTLS, что способно привести к утечке конфиденциальных данных, отправляемых легитимными пользователями.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает транзакции EAP для обнаружения любых устройств, которые не реализуют механизм EAP-TTLS, и запускает сигнал тревоги, чтобы уведомить администраторов об уязвимости. Отображаемый на экране AirWISE текст сигнала тревоги включает идентификацию проблемного устройства, а также используемый альтернативный механизм аутентификации. Мы рекомендуем ИТ-персоналу найти устройство, вызывающее тревогу, и настроить для него использование механизма EAP-TTLS.

AP Using WPA Migration Mode (Точка доступа с использованием режима миграции WPA)

Описание сигнала тревоги и возможные причины

Точки доступа Cisco поддерживают режим миграции WPA (WPA Migration Mode). Это дает возможность клиентам WEP и WPA связываться с точкой доступа, использующей тот же идентификатор SSID. Следующие типы клиентских устройств могут подключаться к точке доступа, используя тот же SSID:

- Клиенты WPA с поддержкой TKIP (Протокол ограниченной по времени целостности ключа) и управлением аутентифицированными ключами.
- Клиенты 802.1X-2001 (такие как устаревшие клиенты LEAP и использующие TLS клиенты, имеющие возможность управления аутентифицированными ключами, но не TKIP).
- Клиенты Static-WEP, не поддерживающие TKIP или управление аутентифицированными ключами.

Режим миграции WPA раскрывает протокол WEP, который имеет множество недостатков. Это позволяет хакерам запустить классическую атаку WEP, чтобы получить ключ WEP и доступ к беспроводной сети. Эта атака в настоящее время встроена в популярный набор беспроводных инструментов Aircrack-ng.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer контролирует среду WLAN и предупреждает администратора сети WLAN, если обнаруживает одну или несколько точек доступа Cisco, работающих в режиме миграции WPA. Режим миграции WPA (WPA Migration Mode) должен быть временным. Если режим миграции WPA не требуется, его следует отключить.

Brute Force Hidden SSID (Получение скрытого идентификатора SSID методом грубой силы)

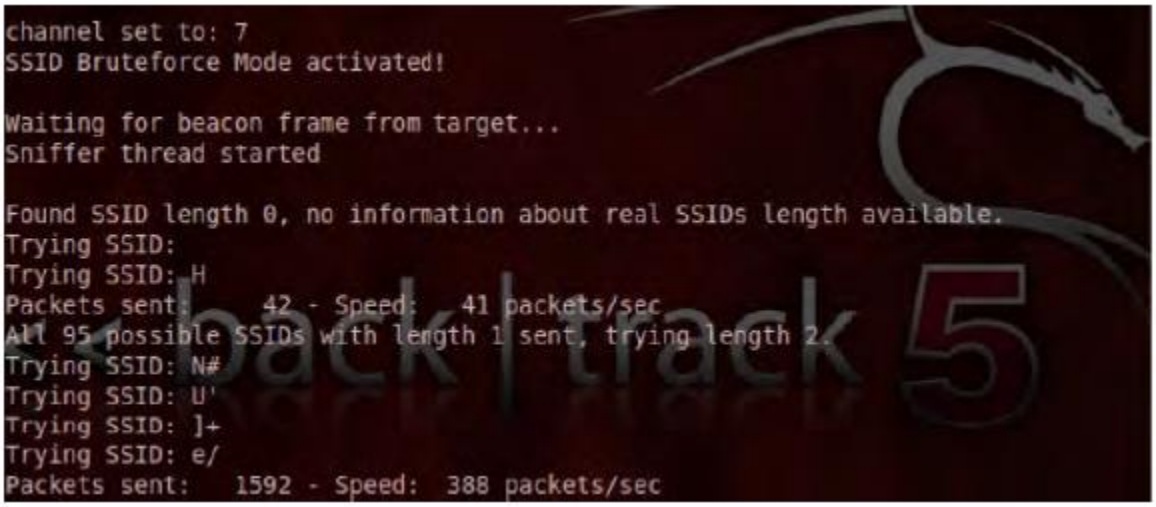
Описание сигнала тревоги и возможные причины

Обычной практикой среди администраторов WLAN является отключение широковещательной передачи идентификатора SSID точкой доступа. Идея заключается в том, что если люди, ищущие беспроводные сети, не видят вас, значит, вы в безопасности. Обычно для подключения к такой беспроводной сети нужно знать идентификатор SSID. Это защищает вашу беспроводную сеть от случайного использования пользователями, у которых нет инструментов извлечения SSID из скрытых сетей. Но хакеры - другое дело. У них есть инструменты, время и энергия для извлечения идентификаторов SSID из скрытых сетей. Существует много инструментов для проведения такого типа отслеживаний. Если скрытый идентификатор SSID не может быть найден обычными методами, хакеры для извлечения SSID скрытой сети могут использовать метод грубой силы для выполнения атаки по словарю или атаки по списку слов.

AP with hidden SSID “abc”	Точка доступа со скрытым идентификатором SSID «abc»
Beacon without SSID	Сигнал маяка без SSID
Response to “abc”	Ответ на «abc»
Probe “a”	Зондирование «a»
Probe “ab”	Зондирование «ab»
Probe “abc”	Зондирование «abc»

Обычно используемые инструменты

Mdk3 - это популярный инструмент DoS-атаки на сеть WLAN, который может выполнять множество различных типов беспроводных атак. Одной из них является режим ESSID Bruteforcing. В этом режиме Mdk3 использует словарь символов для проверки различных комбинаций идентификаторов SSID, ожидая ответа от точки доступа.



Решение AirMagnet

Приложение AirMagnet Enterprise контролирует беспроводную сеть на наличие потенциального трафика, который соответствует атаке методом грубой силы против скрытого SSID, и уведомляет администратора сети WLAN. Персоналу службы безопасности рекомендуется идентифицировать устройство и определять его местонахождение с помощью экрана Floor Plan (План этажа). Атакующую станцию следует как можно скорее удалить из беспроводной среды.

Device Unprotected by any Selected Authentication Methods (Устройство не защищено какими-либо методами аутентификации)

Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer отслеживает транзакции 802.1x и их конкретные методы EAP (Extensible Authentication Protocol – Протокол расширенной аутентификации). Когда конкретный метод EAP не используется, это вызывает подачу сигнала тревоги.

Для этого сигнала тревоги приложение AirMagnet Wi-Fi Analyzer поддерживает следующие методы EAP.

- LEAP – Это собственный метод EAP, разработанный компанией Cisco. Решение Cisco LEAP обеспечивает взаимную аутентификацию, динамическую для каждого сеанса и для каждого пользовательского ключа, а также настраиваемый таймаут сеансового ключа WEP.
- PEAP – Protected Extensible Authentication Protocol (Защищенный протокол расширенной аутентификации), также известный как защищенный протокол EAP. Этот протокол инкапсулирует EAP в потенциально зашифрованный и аутентифицированный туннель безопасности транспортного уровня (Transport Layer Security - TLS).
- EAP-TLS - Extensible Authentication Protocol - Transport Layer Security (Безопасность транспортного уровня протокола расширенной аутентификации). Механизм EAP-TLS обеспечивает дополнительную безопасность по сравнению со стандартными сеансами аутентификации с совместно используемым ключом и паролем, создавая новый ключ для каждого сеанса.
- EAP-TTLS - Extensible Authentication Protocol -Tunneled Transport Layer Security (EAP-TTLS). Это протокол EAP, расширяющий TLS. EAP-TTLS обеспечивает такую же надежную безопасность, как EAP-TLS, но не требует выдачи сертификатов клиентам. Аутентификация пользователя по-прежнему выполняется с помощью паролей, но учетные данные туннелируются.
- EAP-FAST - Cisco Systems разработала протокол расширенной аутентификации с гибкой аутентификацией через протокол безопасного туннелирования (EAP-FAST). В EAP-FAST между клиентом и сервером создается туннель с использованием PAC (Защищенного доступа) для аутентификации друг друга. После процесса установления туннеля клиент аутентифицируется с использованием учетных данных – имени пользователя и пароля.
- EAP-MD5 - это метод аутентификации на основе пароля, обеспечивающий минимальную безопасность. EAP-MD5 отличается от других методов EAP тем, что он обеспечивает только аутентификацию одноранговой узла EAP на сервере EAP, но не взаимную аутентификацию.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает транзакции EAP для обнаружения любых устройств, которые не реализуют включенные методы аутентификации, и запускает сигнал тревоги, чтобы уведомить администраторов об уязвимости. Отображаемый на экране AirWISE текст сигнала тревоги идентифицирует проблемное устройство. ИТ-персоналу рекомендуется найти устройство, вызывающее тревогу, и настроить на нем использование правильного метода аутентификации.

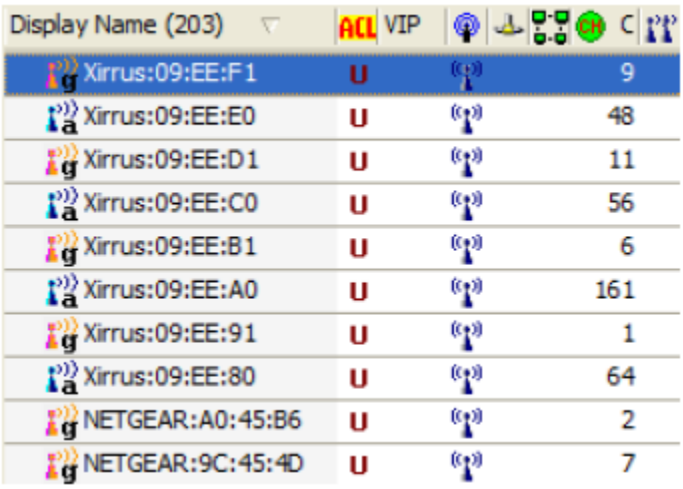
Device with Invalid IEEE OUI (Устройство с недопустимым уникальным идентификатором организации IEEE)

Описание сигнала тревоги и возможные причины

OUI (уникальный идентификатор организации) производителя - это 24-битный номер, который приобретается в IEEE (Институт инженеров по электротехнике и радиоэлектронике) и способен идентифицировать поставщика или производителя по блоку назначенных адресов. В 802.11 это будет

MAC-адрес устройства. Компании покупают блоки адресов, чтобы присвоить им свой идентификатор компании.

AirMagnet Enterprise запрашивает список OUI с веб-сайта IEEE один раз в день и выгружает OUI любого нового производителя в датчики. Когда устройства обнаруживаются и выгружаются на сервер AirMagnet Enterprise, MAC-адреса преобразуются в OUI производителя для более легкой идентификации для конечного пользователя.



Display Name (203)	ACL	VIP	C
Xirrus:09:EE:F1	U		9
Xirrus:09:EE:E0	U		48
Xirrus:09:EE:D1	U		11
Xirrus:09:EE:C0	U		56
Xirrus:09:EE:B1	U		6
Xirrus:09:EE:A0	U		161
Xirrus:09:EE:91	U		1
Xirrus:09:EE:80	U		64
NETGEAR:A0:45:B6	U		2
NETGEAR:9C:45:4D	U		7

Если MAC-адреса не найдены в базе данных производителей IEEE, это достаточно надежный признак того, что MAC-адрес для этого устройства был динамически сгенерирован, а не назначен производителем. Это может указывать на возможную атаку, поскольку большинство хакеров перед началом атаки изменяют MAC-адрес своей беспроводной карты, чтобы их было сложнее идентифицировать.

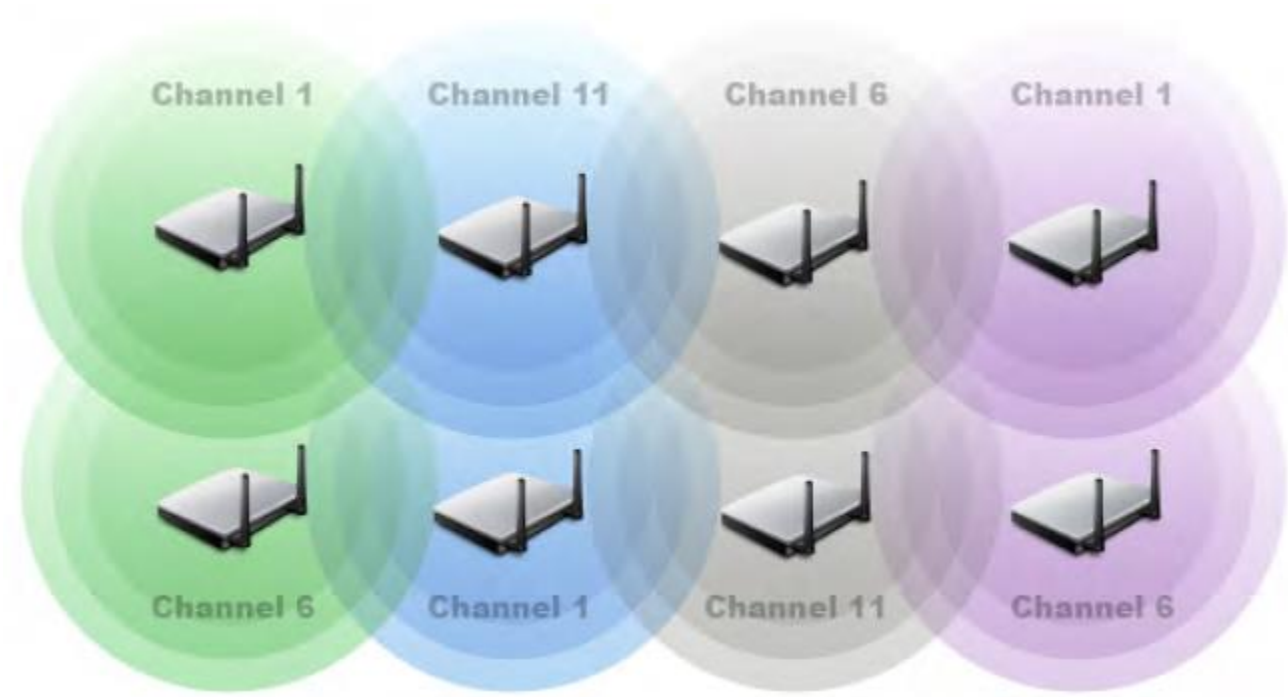
Решение AirMagnet

Датчики AirMagnet Smartedge сканируют сеть WLAN в поиске устройств с MAC-адресами, не имеющими назначенного идентификатора производителя (Vendor OUI). При обнаружении такого нарушения AirMagnet Enterprise предупреждает о нем администратора WLAN. Рекомендуется найти устройство, чтобы определить его легитимность.

Channel With Overloaded APs (Канал с перегруженными точками доступа)

Описание сигнала тревоги и возможные причины

Радиочастотный спектр - это общедоступная среда, в которой работающие в одном канале (на одной радиочастоте) устройства (802.11a, 11b или 11g) совместно используют его полосу пропускания. Распределяется не только полоса пропускания; каналы с большим количеством устройств имеют более высокую вероятность коллизий при передаче, проблем со скрытыми узлами, помех и т.д. Во избежание помех в совмещенном канале проведение типового обследования площадки позволит назначить физически соседним точкам доступа неперекрывающиеся каналы. На рисунке ниже показан пример распределения каналов для находящихся рядом точек доступа.

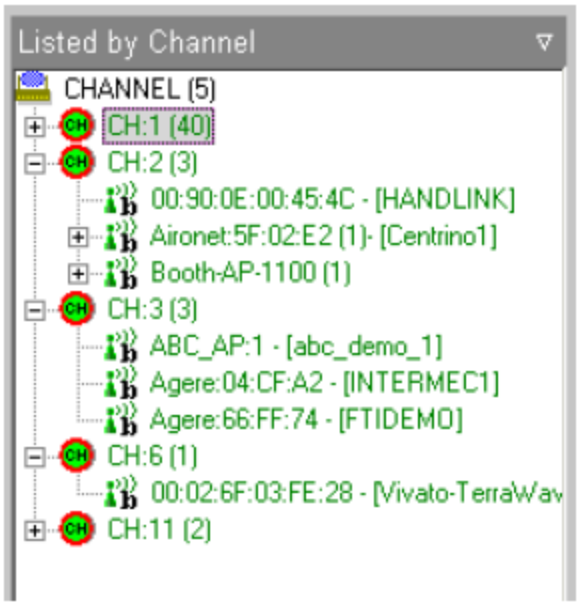


Channel	Канал

Обследование площадки позволяет выделить физически смежным точкам доступа неперекрывающиеся каналы

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает выделение и использование каналов и подает этот сигнал тревоги, когда количество точек доступа на канале превышает предварительно заданное максимальное значение (настраиваемый порог срабатывания сигнализации равен 3). Этот сигнал тревоги учитывает только точки доступа, работающие в одном и том же канале. Другой сигнал тревоги приложения AirMagnet WiFi Analyzer (точки доступа с взаимными помехами) анализирует помехи, создаваемые точками доступа, которые работают в соседних каналах. Для дальнейшего изучения текущего использования канала и принятия соответствующих мер пользователи могут использовать экран Infrastructure (Инфраструктура) приложения AirMagnet WiFi Analyzer (смотрите рисунок ниже).



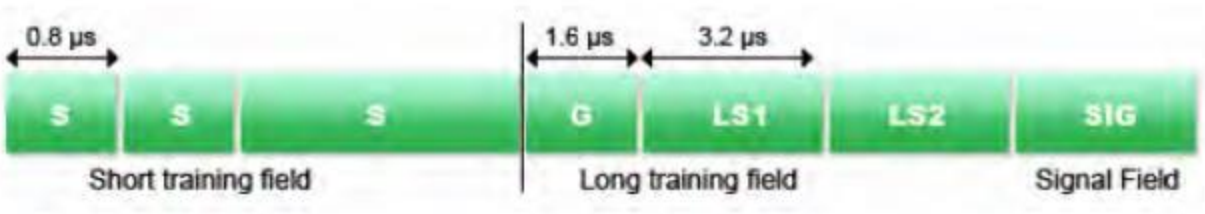
На экране инфраструктуры (список по каналам) показано распределение каналов.

Overlapping Legacy BSS Condition (OLBC) Exists on Channel (На канале существует состояние OLBC (Состояние перекрывающихся устаревших основных наборов служб))

Описание сигнала тревоги и возможные причины

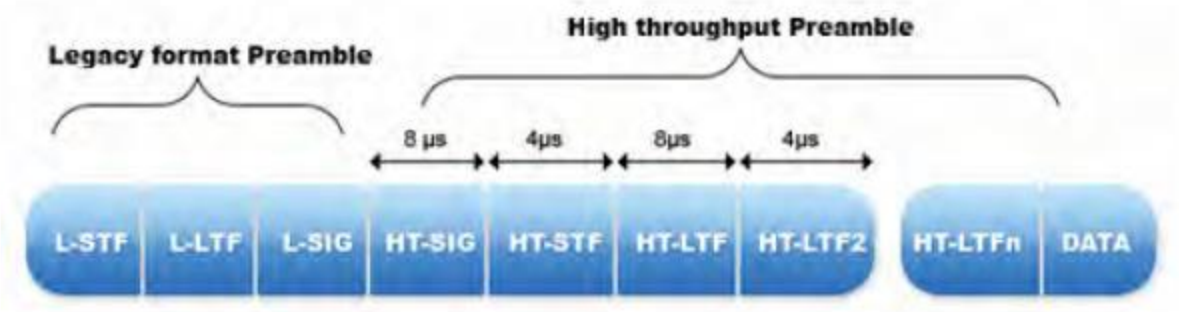
Несмотря на то, что точки доступа 802.11n конструктивно имеют обратную совместимость со станциями, построенными с использованием устаревших стандартов 802.11a/b/g, пользователи 802.11n обладают возможностью работать в так называемом режиме Greenfield. Развертывание 802.11n Greenfield - это сеть 802.11n, развернутая и работающая таким образом, что обратная совместимость с устаревшими устройствами 802.11a/b/g не требуется. Это наиболее эффективный режим сети 802.11n, поскольку он позволяет полностью использовать набор функций 802.11n. Если требуется защита устаревших устройств, нужно будет пожертвовать скоростью передачи данных как на уровне PHY, так и на уровне MAC стандарта 802.11n.

Когда необходима защита устаревших устройств, на уровне PHY устройства 802.11n должны передавать преамбулу смешанного режима даже при передаче в режиме HT (802.11n High Throughput). Преамбула смешанного режима по существу является преамбулой устаревшего формата, за которой следует преамбула HT. Это позволяет устаревшим станциям, которые не понимают преамбулу HT, по-прежнему распознавать передачу и откладывать использование среды. В развертывании Greenfield используется только преамбула HT:



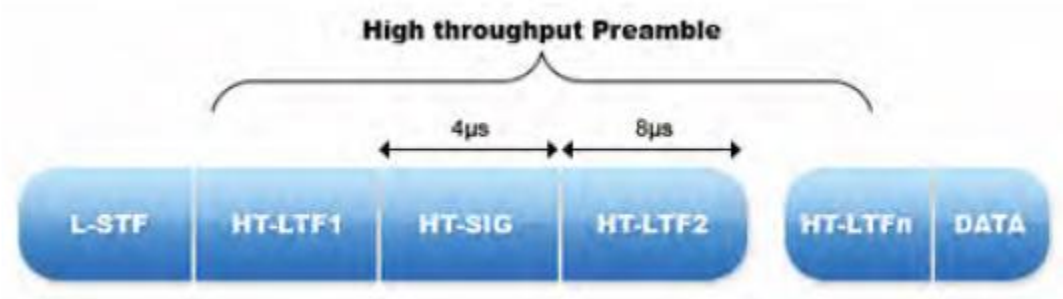
µs	мкс
Short training field	Короткое обучающее поле
Long training field	Длинное обучающее поле
Signal Field	Поле сигнала

Преамбула устаревшего формата



Legacy formal Preamble	Преамбула устаревшего формата
High throughput Preamble	Преамбула высокой пропускной способности
µs	мкс

Преамбула смешанного режима



High throughput Preamble	Преамбула высокой пропускной способности
µs	мкс

Преамбула режима HT

Еще на большие уступки приходится идти на уровне MAC, так как передачам 802.11n в режиме HT должны предшествовать низкоскоростные обмены кадрами устаревшего формата CTS-to-self, RTS/CTS или аналогичными, чтобы в устаревших узлах заработали механизмы контроля виртуальной несущей. Устаревшие узлы обновляют свой вектор распределения сети (NAV), который используется для виртуального определения того, когда среда снова станет свободной, на основе полей Duration/ID в этих кадрах. Это значит, когда требуется защита, передача в режиме HT (потенциально) использует больше времени для кадров «защиты», чем для собственных данных. Несмотря на то, что кадры типа RTS и CTS относительно короткие, для обмена кадрами RTS/CTS с устаревшей скоростью 6 Мбит/с потребуется больше времени, чем для передачи 500 байтов с максимальной скоростью передачи данных 802.11n.

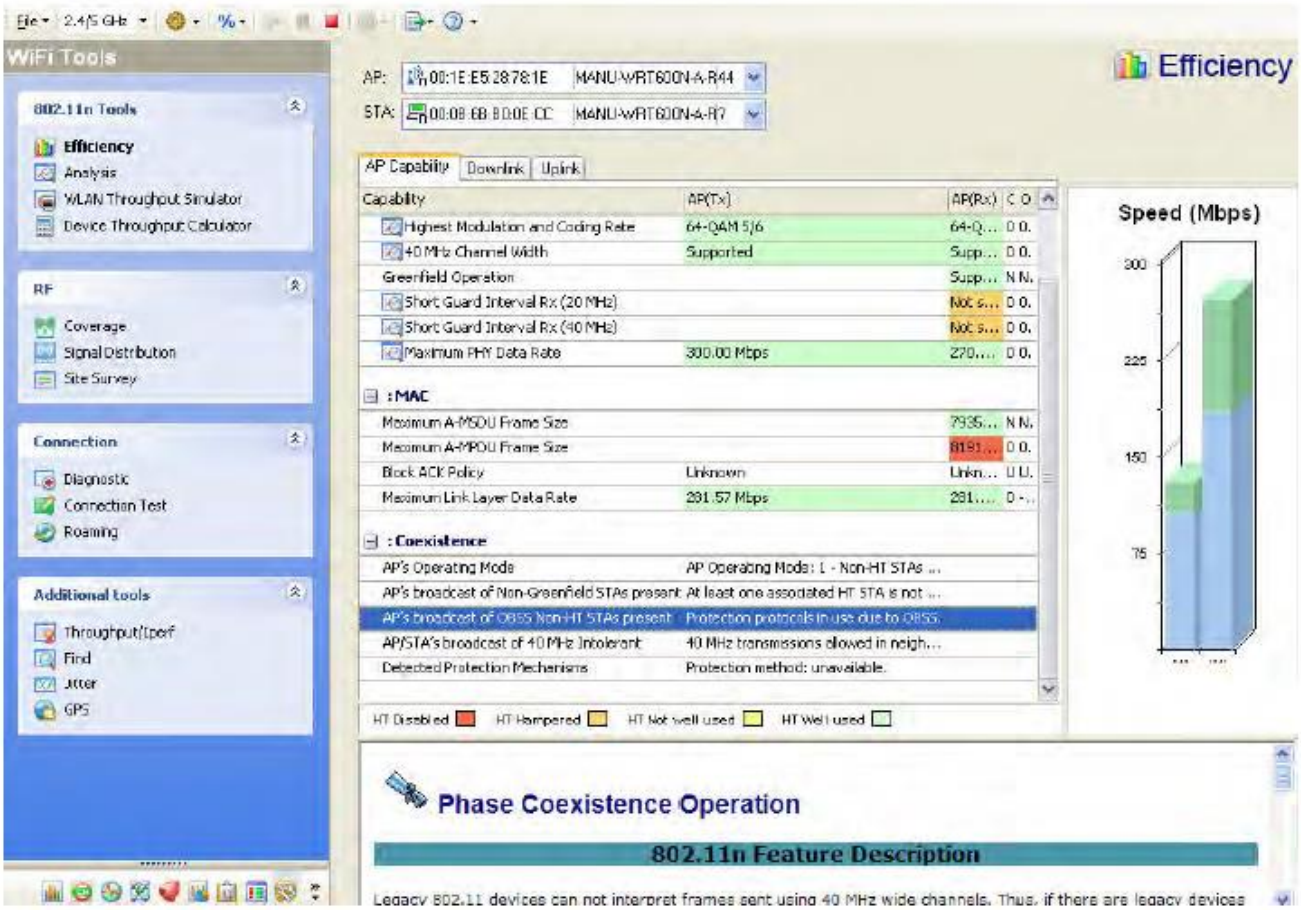
Следует отметить, что для начала действия этих механизмов защиты устаревшая станция даже не должна быть связана с BSS 802.11n. Просто присутствие кадров от устаревших устройств заставляет сети 802.11n Greenfield понижать производительность до работы в смешанном режиме.

OLBC (Overlapping Legacy BSS Condition) относится к ситуации, в которой устаревший (то есть 802.11a/b/g) основной набор служб (BSS) обнаруживается поблизости от основного набора служб 802.11n в той степени, в которой точка доступа 802.11n может слышать сигналы маяка от соседнего BSS.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer оповещает канал, когда обнаруживает сигналы маяка от устаревшего BSS, работающего в пределах дальности действия точки доступа HT (точка доступа реализует механизмы защиты, как описано выше) на этом канале или на перекрывающемся канале. AirMagnet рекомендует, чтобы сети 802.11n и устаревшие сети были физически разделены или, как минимум, работали на разных каналах.

Инструмент Efficiency (Эффективность) приложения AirMagnet WiFi Analyzer проводит анализ возможностей точки доступа 802.11n и информирует пользователя о любых проблемах сосуществования с устаревшими устройствами 802.11 a/b/g.



Инструмент Efficiency (Эффективность) приложения AirMagnet WiFi Analyzer указывает на проблемы сосуществования

AirMagnet предупреждает пользователя о нескольких проблемах сосуществования, таких как:
1. В основном или дополнительном канале присутствуют станции не HT (Non-HT Station).
2. Имеются подключенные станции, которые не поддерживают Greenfield.
3. В перекрывающемся BSS есть станции не HT (Non-HT Station).
4. Перекрывающиеся BSS допускают передачу 40 МГц.

Пользователи приложения AirMagnet WiFi Analyzer также могут просматривать сводную информацию о сосуществовании (например, информацию об обнаруженных станциях «Non-HT» и т.д.) для точек доступа 802.11n, выбрав на экране Start опцию Easy View > View by 802.11n (Легкий просмотр > Просмотр по 802.11n).

SGI	2nd Ch	STA Ch Width	Operating Mode	Non-Greenfield STA ...	OBSS	RIFS Mode	PCO				SM P
	Above	Any	Non-HT STAs present	1	Y	permitted	N	N	0	N	SM e
20/40	None	20	Non-HT STAs present	1	N	Prohibited	N	N	0	N	SM e
20/40	Below	Any	Non-HT STAs present	1	N	Prohibited	N	N	0	N	SM e
40	Below	Any	Non-HT STAs present	0	N	Prohibited	N	N	0	N	SM e
40	None	20	Non-HT STAs present	0	Y	Prohibited	N	N	0	N	SM e
	Below	Any	One ore more non-HT S...	0	Y	Prohibited	N	N	0	N	SM e
	Above	Any	Non-HT STAs present	0	Y	permitted	N	N	0	N	SM e
20	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
	Below	Any	Non-HT STAs present	0	Y	permitted	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e
20	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	Stati
	None	20	All STAs HT	0	N	Prohibited	N	N	0	N	SM e

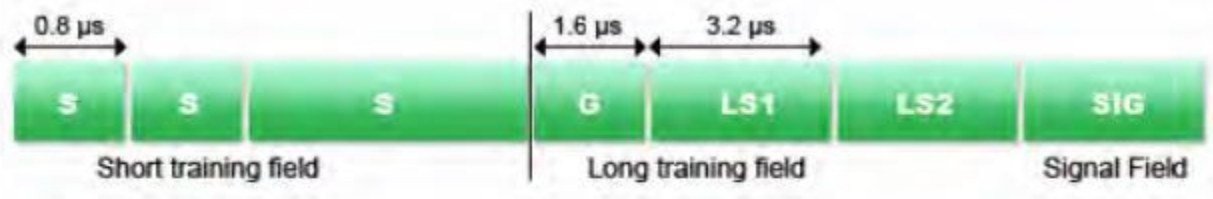
Экран Easy View 802.11n приложения AirMagnet Wi-Fi Analyzer

HT-Enabled AP with OLBC (Точка доступа с поддержкой HT и OLBC)

Описание сигнала тревоги и возможные причины

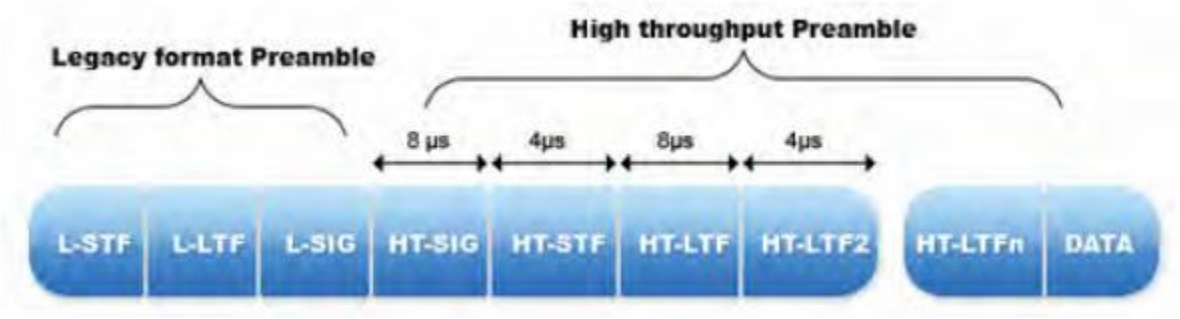
Несмотря на то, что точки доступа 802.11n конструктивно имеют обратную совместимость со станциями, построенными с использованием устаревших стандартов 802.11a/b/g, пользователи 802.11n обладают возможностью работать в так называемом режиме Greenfield. Развертывание 802.11n Greenfield - это сеть 802.11n, развернутая и работающая таким образом, что обратная совместимость с устаревшими устройствами 802.11a/b/g не требуется. Это наиболее эффективный режим сети 802.11n, поскольку он позволяет полностью использовать набор функций 802.11n. Если требуется защита устаревших устройств, нужно будет пожертвовать скоростью передачи данных как на уровне PHY, так и на уровне MAC стандарта 802.11n.

Когда необходима защита устаревших устройств, на уровне PHY устройства 802.11n должны передавать преамбулу смешанного режима даже при передаче в режиме HT (802.11n High Throughput). Преамбула смешанного режима по существу является преамбулой устаревшего формата, за которой следует преамбула HT. Это позволяет устаревшим станциям, которые не понимают преамбулу HT, по-прежнему распознавать передачу и откладывать использование среды. В развертывании Greenfield используется только преамбула HT:



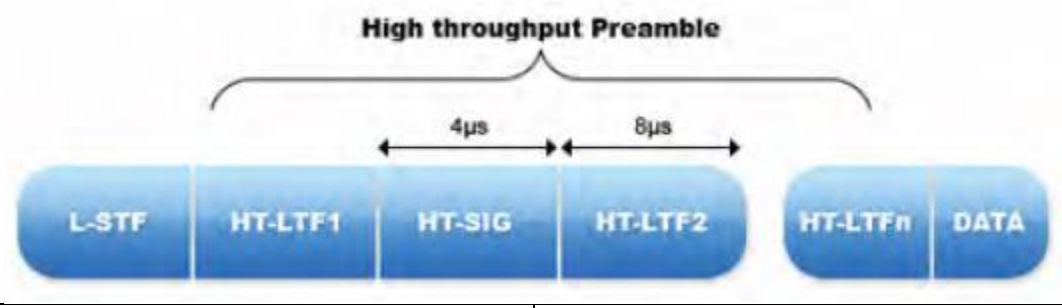
µs	мкс
Short training field	Короткое обучающее поле
Long training field	Длинное обучающее поле
Signal Field	Поле сигнала

Преамбула устаревшего формата



Legacy formal Preamble	Преамбула устаревшего формата
High throughput Preamble	Преамбула высокой пропускной способности
µs	мкс

Преамбула смешанного режима



High throughput Preamble	Преамбула высокой пропускной способности
µs	мкс

Преамбула режима HT

Еще на большие уступки приходится идти на уровне MAC, так как передачам 802.11n в режиме HT должны предшествовать низкоскоростные обмены кадрами устаревшего формата CTS-to-self, RTS/CTS или аналогичными, чтобы в устаревших узлах заработали механизмы контроля виртуальной несущей. Устаревшие узлы обновляют свой вектор распределения сети (NAV), который используется для виртуального определения того, когда среда снова станет свободной, на основе полей Duration/ID в этих кадрах. Это значит, когда требуется защита, передача в режиме HT (потенциально) использует больше времени для кадров «защиты», чем для собственных данных. Несмотря на то, что кадры типа RTS и CTS относительно короткие, для обмена кадрами RTS/CTS с устаревшей скоростью 6 Мбит/с потребуется больше времени, чем для передачи 500 байтов с максимальной скоростью передачи данных 802.11n.

Следует отметить, что для начала действия этих механизмов защиты устаревшая станция даже не должна быть связана с BSS 802.11n. Просто присутствие кадров от устаревших устройств заставляет сети 802.11n Greenfield понижать производительность до работы в смешанном режиме.

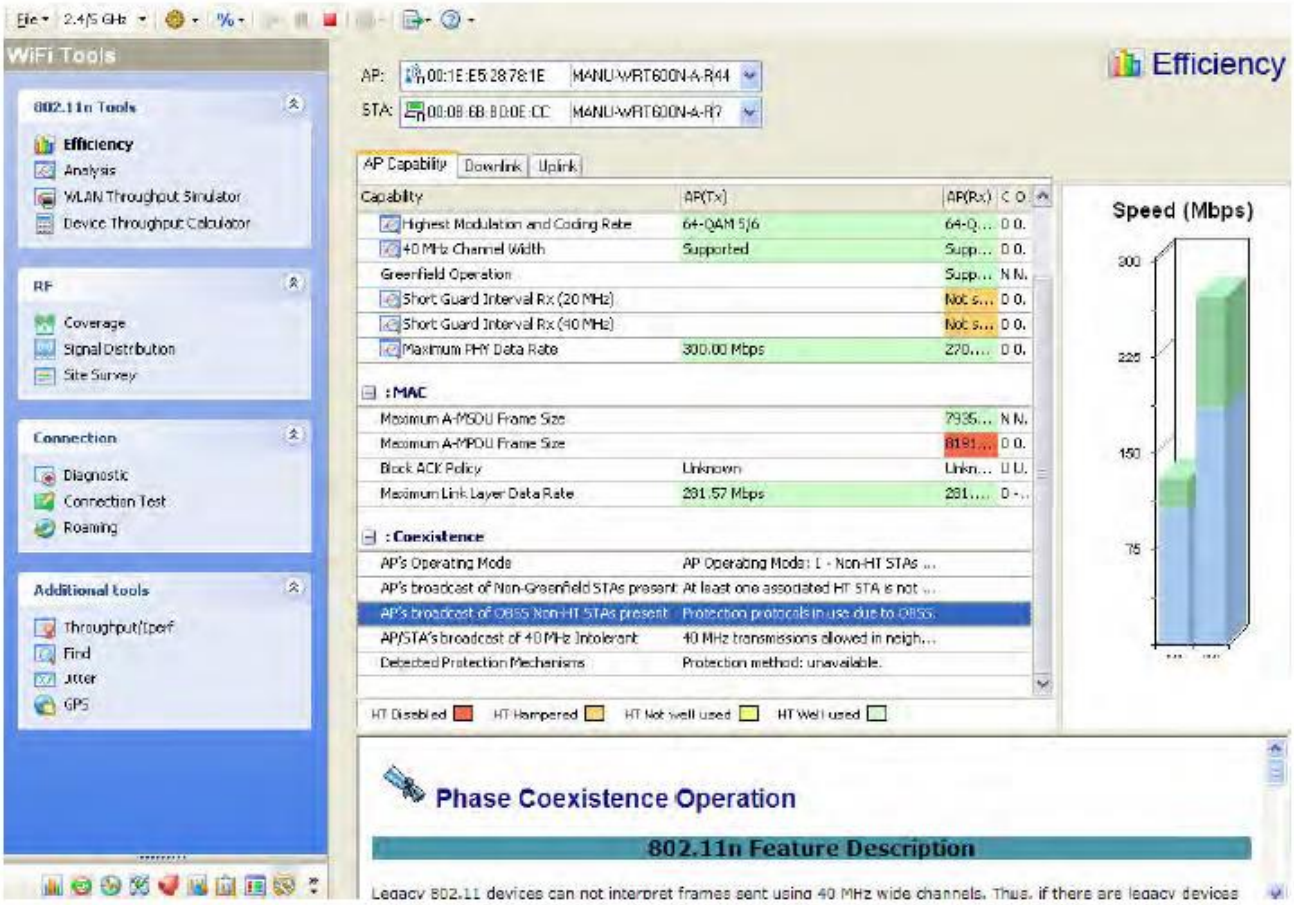
OLBC (Overlapping Legacy BSS Condition) относится к ситуации, в которой устаревший (то есть 802.11a/b/g) основной набор служб (BSS) обнаруживается поблизости от основного набора служб 802.11n в той степени, в которой точка доступа 802.11n может слышать сигналы маяка от соседнего BSS.

Решение AirMagnet

Приложение AirMagnet Wi-Fi Analyzer оповещает точку доступа (реализуя механизмы защиты, как описано выше) и канал, когда обнаруживает сигналы маяка от устаревшего BSS, работающего в пределах радиуса действия точки доступа с поддержкой HT (приложение AirMagnet обнаружило точку доступа, передающую трафик HT) на том же канале или на перекрывающемся канале. По мере реализации механизмов защиты это состояние приводит к потенциальным проблемам с пропускной способностью. AirMagnet рекомендует, чтобы сети 802.11n и устаревшие сети были физически разделены или, как минимум, работали на разных каналах.

Приложение AirMagnet Wi-Fi Analyzer обнаруживает трафик HT от точки доступа 802.11n

Инструмент Efficiency (Эффективность) приложения AirMagnet WiFi Analyzer проводит анализ возможностей точки доступа 802.11n и информирует пользователя о любых проблемах сосуществования с устаревшими устройствами 802.11 a/b/g.



Инструмент Efficiency (Эффективность) приложения AirMagnet WiFi Analyzer указывает на проблемы сосуществования

AirMagnet предупреждает пользователя о нескольких проблемах сосуществования, таких как:

1. В основном или дополнительном канале присутствуют станции не HT (Non-HT Station).
2. Имеются подключенные станции, которые не поддерживают Greenfield.
3. В перекрывающемся BSS есть станции не HT (Non-HT Station).
4. Перекрывающиеся BSS допускают передачу 40 МГц.

Пользователи приложения AirMagnet WiFi Analyzer также могут просматривать сводную информацию о сосуществовании для точек доступа 802.11n, выбрав на экране Start опцию Easy View > View by 802.11n (Легкий просмотр > Просмотр по 802.11n).

SGI	2nd Ch	STA Ch Width	Operating Mode	Non-Greenfield STA ...	OBSS	RIFS Mode	PCO				SM P
	Above	Any	Non-HT STAs present	1	Y	permitted	N	N	0	N	SM e
20/40	None	20	Non-HT STAs present	1	N	Prohibted	N	N	0	N	SM e
20/40	Below	Any	Non-HT STAs present	1	N	Prohibted	N	N	0	N	SM e
40	Below	Any	Non-HT STAs present	0	N	Prohibted	N	N	0	N	SM e
40	None	20	Non-HT STAs present	0	Y	Prohibted	N	N	0	N	SM e
	Below	Any	One ore more non-HT S...	0	Y	Prohibted	N	N	0	N	SM e
	Above	Any	Non-HT STAs present	0	Y	permitted	N	N	0	N	SM e
20	None	20	All STAs HT	0	N	Prohibted	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibted	N	N	0	N	SM e
	Below	Any	Non-HT STAs present	0	Y	permitted	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibted	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibted	N	N	0	N	SM e
	None	20	All STAs HT	0	N	Prohibted	N	N	0	N	SM e
20	None	20	All STAs HT	0	N	Prohibted	N	N	0	N	Stati
	None	20	All STAs HT	0	N	Prohibted	N	N	0	N	SM e

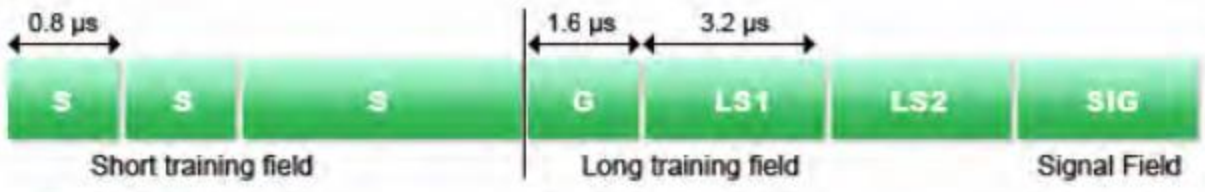
Экран Easy View 802.11n приложения AirMagnet Wi-Fi Analyzer

OLBC Detected on Channel Not Implementing Protection Mechanisms (Состояние OLBC обнаружено на канале, не реализующем механизмы защиты)

Описание сигнала тревоги и возможные причины

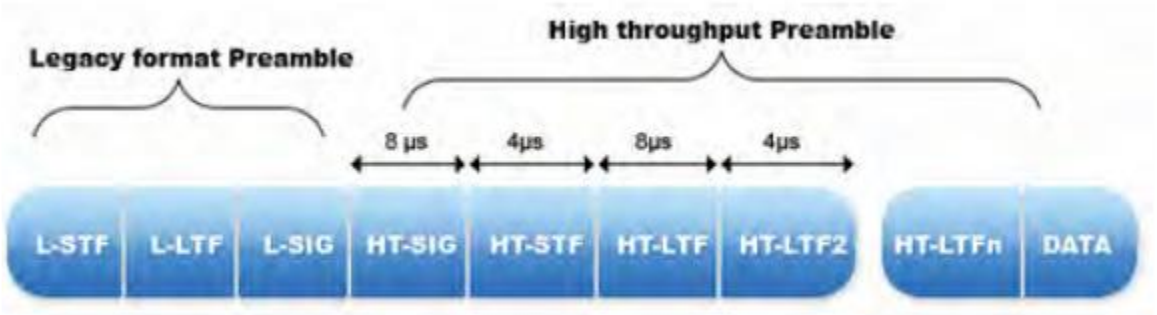
Подобно устройствам 802.11g, которым необходимы механизмы защиты для поддержания обратной совместимости с устройствами 802.11b, устройства 802.11n также должны использовать различные механизмы защиты для защиты своей передачи от устаревших устройств 802.11 a/b/g. Устройства 802.11n передают сигналы, которые непонятны устаревшим устройствам. Чтобы предотвратить коллизии и нежелательные помехи, очень важно, чтобы в сети были реализованы механизмы защиты.

На уровне PHY, когда необходима защита от устаревших устройств, устройства 802.11n должны передавать преамбулу смешанного режима даже при передаче HT (802.11n High Throughput). Преамбула смешанного режима по существу является преамбулой устаревшего формата, за которой следует преамбула HT. Это позволяет устаревшим станциям, которые не понимают преамбулу HT, по-прежнему распознавать передачу и откладывать использование среды. В развертывании Greenfield используется только преамбула HT:



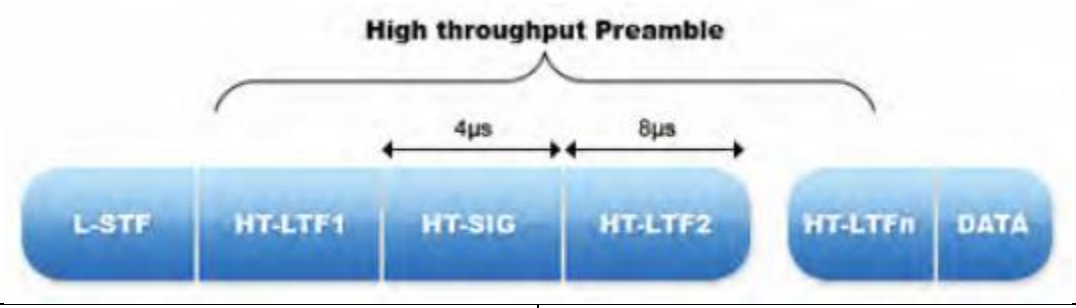
µs	мкс
Short training field	Короткое обучающее поле
Long training field	Длинное обучающее поле
Signal Field	Поле сигнала

Преамбула устаревшего формата



Legacy formal Preamble	Преамбула устаревшего формата
High throughput Preamble	Преамбула высокой пропускной способности
µs	мкс

Преамбула смешанного режима



High throughput Preamble	Преамбула высокой пропускной способности
µs	мкс

Преамбула режима HT

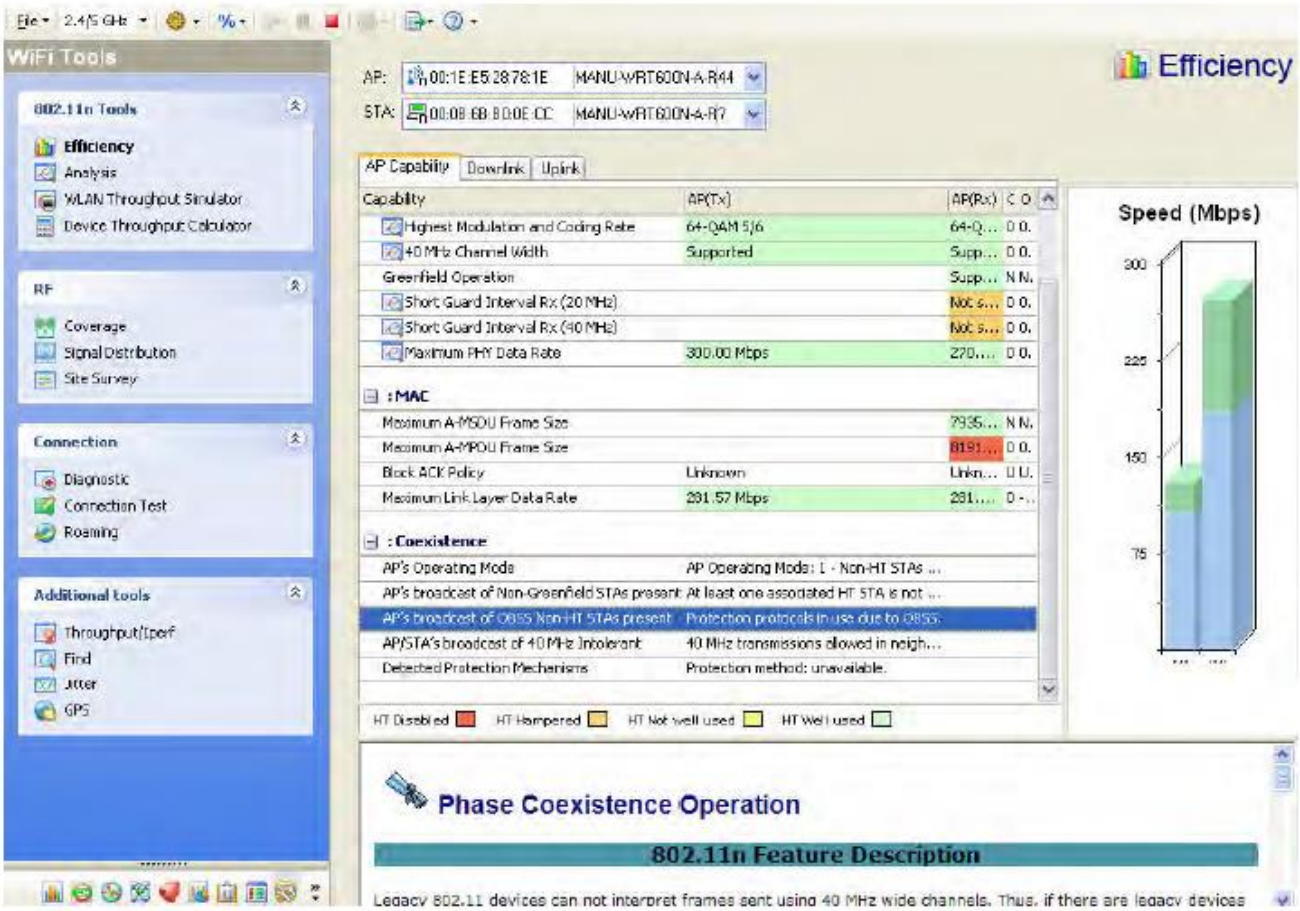
Устаревшие узлы обновляют свой вектор выделения сети (Network Allocation Vector - NAV), который используется для виртуального определения того, когда среда снова станет свободной, на основе полей Duration/ID, присутствующих в этих кадрах. Следует отметить, что для начала действия этих механизмов защиты устаревшая станция даже не должна быть связана с BSS 802.11n.

OLBC (Overlapping Legacy BSS Condition) относится к ситуации, в которой устаревший (то есть 802.11a/b/g) основной набор служб (BSS) обнаруживается поблизости от основного набора служб 802.11n в той степени, в которой точка доступа 802.11n может слышать сигналы маяка от соседнего BSS.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer оповещает канал, когда обнаруживает сигналы маяка от устаревшего BSS, работающего в пределах радиуса действия точки доступа с поддержкой HT (приложение AirMagnet обнаружило точку доступа, передающую трафик HT) на том же канале или на перекрывающемся канале, и что точка доступа не использует никакой механизм защиты для защиты своей передачи от устаревших устройств. AirMagnet рекомендует, чтобы сети 802.11n и устаревшие сети были физически разделены или, как минимум, работали на разных каналах.

Инструмент Efficiency (Эффективность) приложения AirMagnet WiFi Analyzer проводит анализ возможностей точки доступа 802.11n и информирует пользователя о любых проблемах сосуществования с устаревшими устройствами 802.11 a/b/g.



Инструмент Efficiency (Эффективность) приложения AirMagnet WiFi Analyzer указывает на проблемы сосуществования

AirMagnet предупреждает пользователя о нескольких проблемах сосуществования, таких как:

1. В основном или дополнительном канале присутствуют станции не HT (Non-HT Station).
2. Имеются подключенные станции, которые не поддерживают Greenfield.
3. В перекрывающемся BSS есть станции не HT (Non-HT Station).
4. Перекрывающиеся BSS допускают передачу 40 МГц.

Пользователи приложения AirMagnet WiFi Analyzer также могут просматривать сводную информацию о сосуществовании для точек доступа 802.11n, выбрав на экране Start опцию Easy View > View by 802.11n (Легкий просмотр > Просмотр по 802.11n).

	SGI	2nd Ch	STA Ch Width	Operating Mode	Non-Greenfield STA ...	OBSS	RIFS Mode	PCO				SM P
		Above	Any	Non-HT STAs present	1	Y	permitted	N	N	0	N	SM e
	20/40	None	20	Non-HT STAs present	1	N	Prohibted	N	N	0	N	SM e
	20/40	Below	Any	Non-HT STAs present	1	N	Prohibted	N	N	0	N	SM e
	40	Below	Any	Non-HT STAs present	0	N	Prohibted	N	N	0	N	SM e
	40	None	20	Non-HT STAs present	0	Y	Prohibted	N	N	0	N	SM e
		Below	Any	One ore more non-HT S...	0	Y	Prohibted	N	N	0	N	SM e
		Above	Any	Non-HT STAs present	0	Y	permitted	N	N	0	N	SM e
	20	None	20	All STAs HT	0	N	Prohibted	N	N	0	N	SM e
		None	20	All STAs HT	0	N	Prohibted	N	N	0	N	SM e
		Below	Any	Non-HT STAs present	0	Y	permitted	N	N	0	N	SM e
		None	20	All STAs HT	0	N	Prohibted	N	N	0	N	SM e
		None	20	All STAs HT	0	N	Prohibted	N	N	0	N	SM e
		None	20	All STAs HT	0	N	Prohibted	N	N	0	N	SM e
	20	None	20	All STAs HT	0	N	Prohibted	N	N	0	N	Stati
		None	20	All STAs HT	0	N	Prohibted	N	N	0	N	SM e

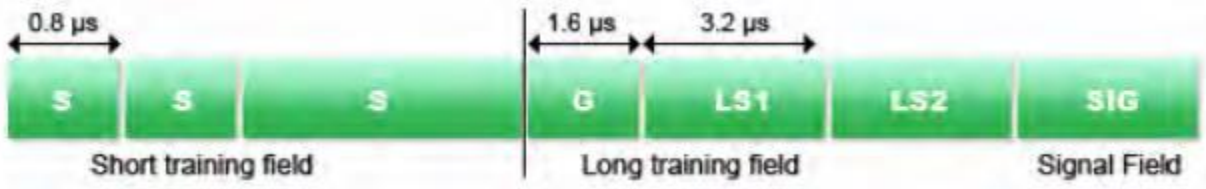
Экран Easy View 802.11n приложения AirMagnet Wi-Fi Analyzer

Non-Required Protection Mechanism Detected (Обнаружен необязательный механизм защиты)

Описание сигнала тревоги и возможные причины

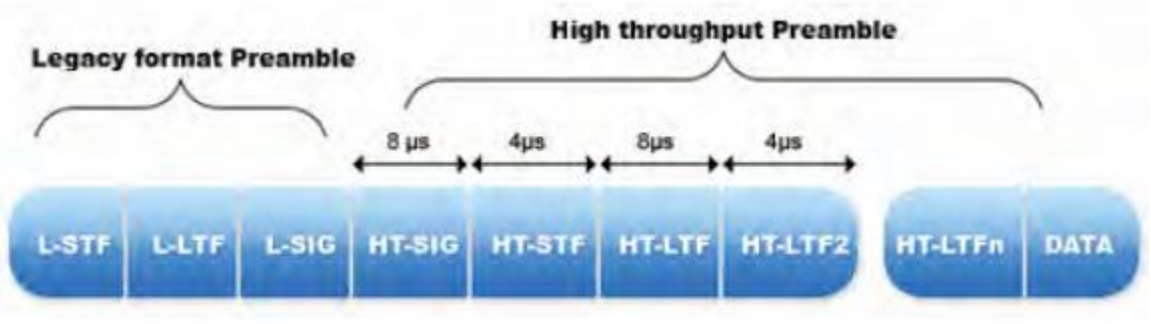
Подобно устройствам 802.11g, которым необходимы механизмы защиты для поддержания обратной совместимости с устройствами 802.11b, устройства 802.11n также должны использовать различные механизмы для защиты своей передачи от устаревших устройств 802.11 a/b/g. Устройства 802.11n передают сигналы, которые непонятны устаревшим устройствам. Чтобы предотвратить коллизии и нежелательные помехи, очень важно, чтобы в сети были реализованы механизмы защиты.

На уровне PHY, когда необходима защита от устаревших устройств, устройства 802.11n должны передавать преамбулу смешанного режима даже при передаче HT (802.11n High Throughput). Преамбула смешанного режима по существу является преамбулой устаревшего формата, за которой следует преамбула HT. Это позволяет устаревшим станциям, которые не понимают преамбулу HT, по-прежнему распознавать передачу и откладывать использование среды. В развертывании Greenfield используется только преамбула HT:



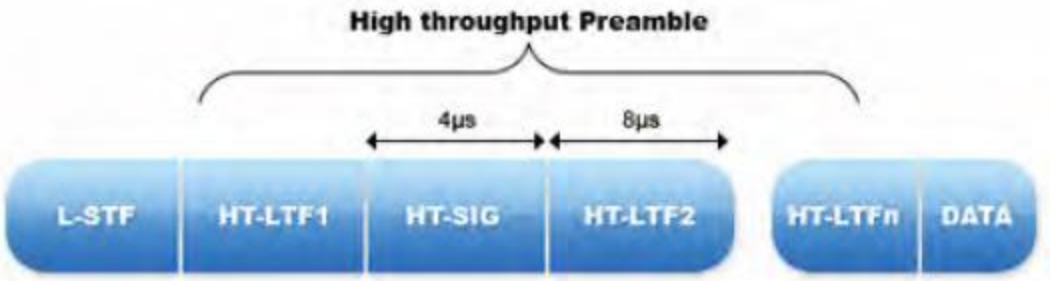
µs	мкс
Short training field	Короткое обучающее поле
Long training field	Длинное обучающее поле
Signal Field	Поле сигнала

Преамбула устаревшего формата



Legacy formal Preamble	Преамбула устаревшего формата
High throughput Preamble	Преамбула высокой пропускной способности
µs	мкс

Преамбула смешанного режима



High throughput Preamble	Преамбула высокой пропускной способности
µs	мкс

Преамбула режима HT

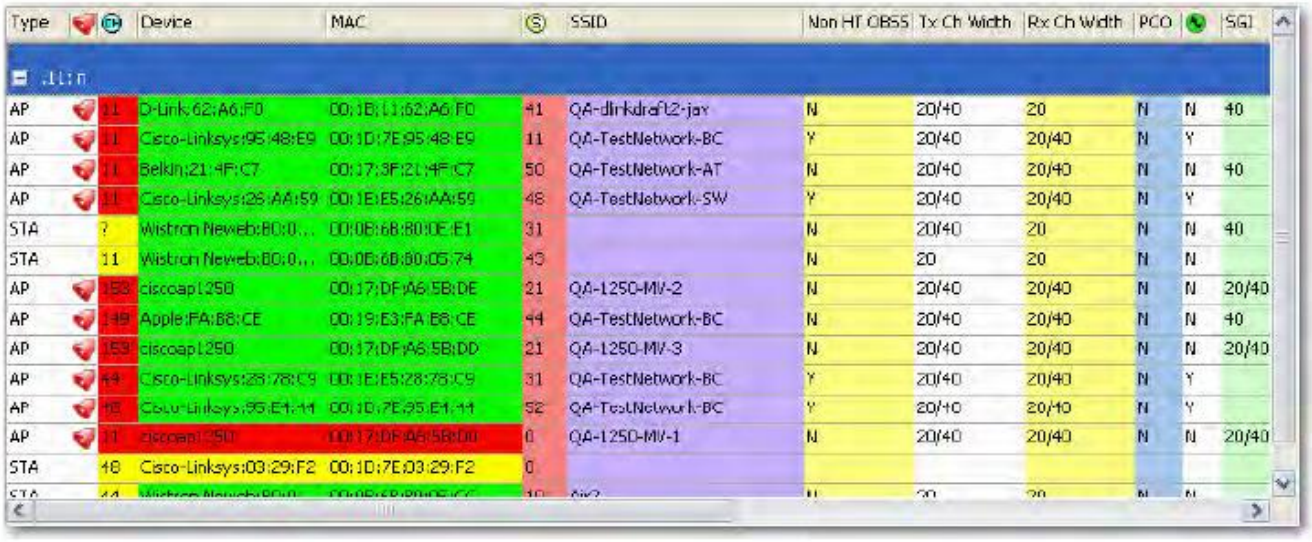
Устаревшие узлы обновляют свой вектор выделения сети (Network Allocation Vector - NAV), который используется для виртуального определения того, когда среда снова станет свободной, на основе полей Duration/ID, присутствующих в этих кадрах. Следует отметить, что устаревшая станция даже не должна быть связана с BSS 802.11n, чтобы эти механизмы защиты начали действовать. Простое присутствие кадров от устаревших устройств заставляет сети 802.11n Greenfield понижать производительность до смешанного режима.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer оповещает точку доступа и канал, когда не обнаруживает устаревшие точки доступа, работающие на том же канале, что и точка доступа с поддержкой HT (AirMagnet обнаруживает точку доступа, передающую трафик HT), но обнаруживает следующие ситуации:

1. Обнаружен механизм защиты, или
2. Сигнал маяка точки доступа сообщает о наличии OBSS станции Non-HT, или
3. Сигнал маяка точки доступа сообщает, что рабочий режим - 1 (станция Non-HT присутствует в первичном или вторичном канале).

Пользователи приложения AirMagnet WiFi Analyzer также могут просматривать сводную информацию о сосуществовании для точек доступа 802.11n, выбрав на экране Start опцию Easy View > View by 802.11n (Легкий просмотр > Просмотр по 802.11n).



Type		Device	MAC		SSID	Non HT OBSS	Tx Ch Width	Rx Ch Width	PCO		SGI
11n											
AP	11	D-Link:62:A6:F0	00:1B:11:62:A6:F0	41	QA-dlinkdraft2-jax	N	20/40	20	N	N	40
AP	11	Cisco-Linksys:95:48:E9	00:1D:7E:95:48:E9	11	QA-TestNetwork-BC	Y	20/40	20/40	N	Y	
AP	11	Belkin:21:4F:C7	00:17:3F:21:4F:C7	50	QA-TestNetwork-AT	N	20/40	20/40	N	N	40
AP	11	Cisco-Linksys:26:AA:59	00:1E:E5:26:AA:59	48	QA-TestNetwork-SW	Y	20/40	20/40	N	Y	
STA	?	Wistron Neweb:80:0...	00:0B:6B:80:0E:E1	31		N	20/40	20	N	N	40
STA	11	Wistron Neweb:80:0...	00:0B:6B:80:05:74	45		N	20	20	N	N	
AP	153	ciscoap1250	00:17:DF:A6:5B:DE	21	QA-1250-MV-2	N	20/40	20/40	N	N	20/40
AP	149	Apple:FA:B6:CE	00:19:E3:FA:B6:CE	44	QA-TestNetwork-BC	N	20/40	20/40	N	N	40
AP	153	ciscoap1250	00:17:DF:A6:5B:DD	21	QA-1250-MV-3	N	20/40	20/40	N	N	20/40
AP	44	Cisco-Linksys:28:78:C9	00:1E:E5:28:78:C9	31	QA-TestNetwork-BC	Y	20/40	20/40	N	Y	
AP	48	Cisco-Linksys:95:E1:11	00:1D:7E:95:E1:11	52	QA-TestNetwork-BC	Y	20/40	20/40	N	Y	
AP	11	ciscoap1250	00:17:DF:A6:5B:D0	0	QA-1250-MV-1	N	20/40	20/40	N	N	20/40
STA	48	Cisco-Linksys:03:29:F2	00:1D:7E:03:29:F2	0							

Экран Start, на котором показаны точки доступа с присутствующими станциями OBSS Non-HT

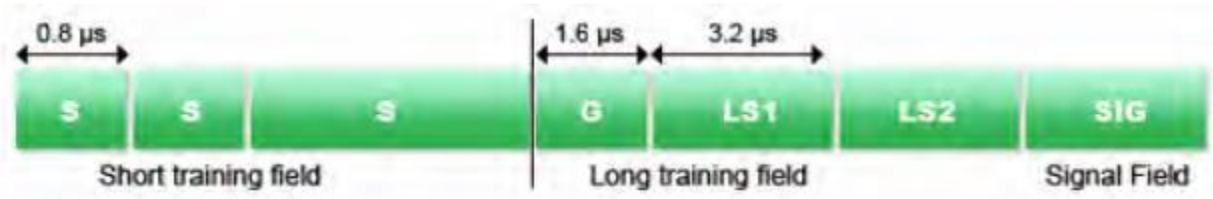
AP Operating in Mixed-Mode (Точка доступа, работающая в смешанном режиме)

Описание сигнала тревоги и возможные причины

Пользователи 802.11n имеют возможность работать в так называемом режиме Greenfield, когда сеть 802.11n развернута и работает таким образом, что обратная совместимость с устаревшими устройствами 802.11a/b/g не требуется. Это наиболее эффективный режим сети 802.11n, поскольку он позволяет полностью использовать набор функций 802.11n. Если требуется защита устаревших устройств, нужно будет пожертвовать скоростью передачи данных как на уровне PHY, так и на уровне MAC стандарта 802.11n.

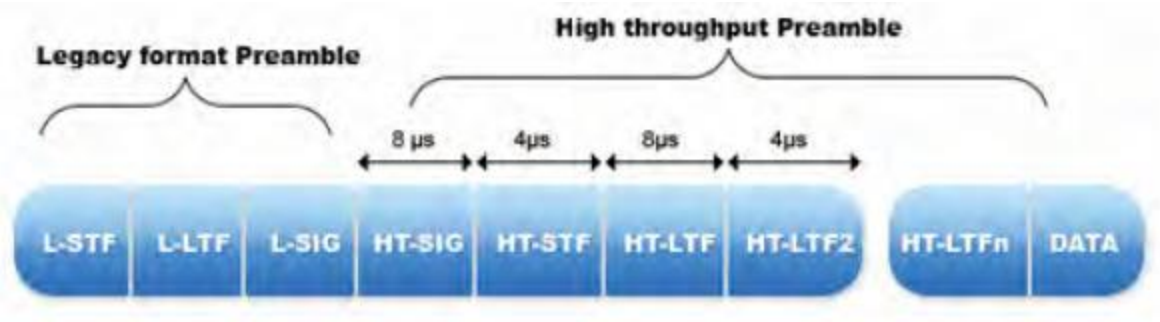
Однако в течение следующего года или около того наиболее распространенным режимом работы точки доступа 802.11n будет обязательный режим HT Mixed. В этом режиме улучшения режима HT могут использоваться одновременно с механизмами защиты HT, которые разрешают связь с устаревшими станциями. Смешанный режим HT (HT Mixed) обеспечивает обратную совместимость, но устройства 802.11n значительно теряют в пропускной способности по сравнению с режимом Greenfield.

На уровне PHY, когда необходима защита от устаревших устройств, устройства 802.11n должны передавать преамбулу смешанного режима даже при передаче HT (802.11n High Throughput). Преамбула смешанного режима по существу является преамбулой устаревшего формата, за которой следует преамбула HT. Это позволяет устаревшим станциям, которые не понимают преамбулу HT, по-прежнему распознавать передачу и откладывать использование среды. В развертывании Greenfield используется только преамбула HT:



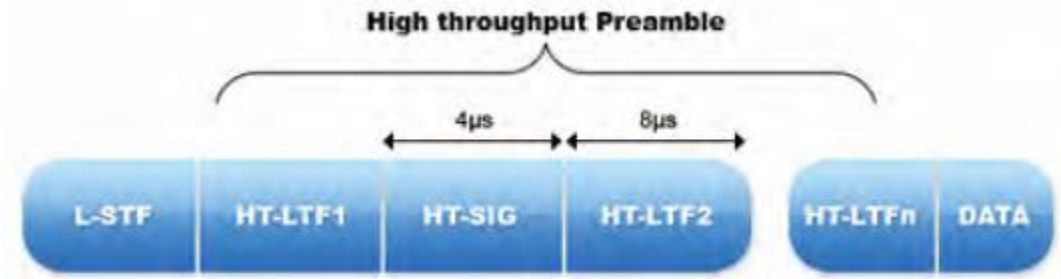
µs	мкс
Short training field	Короткое обучающее поле
Long training field	Длинное обучающее поле
Signal Field	Поле сигнала

Преамбула устаревшего формата



Legacy formal Preamble	Преамбула устаревшего формата
High throughput Preamble	Преамбула высокой пропускной способности
µs	мкс

Преамбула смешанного режима



High throughput Preamble	Преамбула высокой пропускной способности
µs	мкс

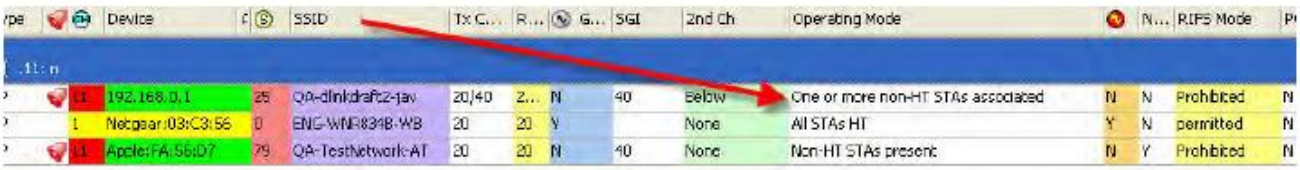
Преамбула режима HT

Еще на большие уступки приходится идти на уровне MAC, так как передачам 802.11n в режиме HT должны предшествовать низкоскоростные обмены кадрами устаревшего формата CTS-to-self, RTS/CTS или аналогичными, чтобы в устаревших узлах заработали механизмы контроля виртуальной несущей. Устаревшие узлы обновляют свой вектор распределения сети (NAV), который используется для виртуального определения того, когда среда снова станет свободной, на основе полей Duration/ID в этих кадрах. Это значит, когда требуется защита, передача в режиме HT (потенциально) использует больше времени для кадров «защиты», чем для собственных данных. Несмотря на то, что кадры типа RTS и CTS относительно короткие, для обмена кадрами RTS/CTS с устаревшей скоростью 6 Мбит/с потребуется больше времени, чем для передачи 500 байтов с максимальной скоростью передачи данных 802.11n.

Следует отметить, что для начала действия этих механизмов защиты устаревшая станция даже не должна быть связана с BSS 802.11n. Просто присутствие кадров от устаревших устройств заставляет сети 802.11n Greenfield понижать производительность до работы в смешанном режиме.

Решение AirMagnet

Когда AirMagnet обнаруживает, что точка доступа указывает рабочий режим, равный 3 (одна или несколько подключенных станций non-HT), либо обнаруживает подключенные к точке доступа станции non-HT, то предупреждает о точке доступа и ее рабочем канале.



Экран Easy View 802.11n приложения AirMagnet Wi-Fi Analyzer, на котором показана точка доступа с подключенными станциями non-HT

Пользователи приложения AirMagnet WiFi Analyzer могут получить эту информацию для точек доступа 802.11n, выбрав на экране Start опцию Easy View > View by 802.11n (Легкий просмотр > Просмотр по 802.11n).

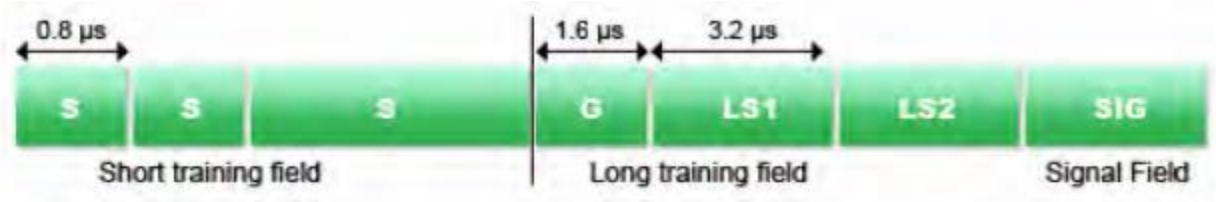
Mixed Mode AP Not Implementing Protection Mechanism (Точка доступа смешанного режима не реализует механизм защиты)

Описание сигнала тревоги и возможные причины

Пользователи 802.11n имеют возможность работать в так называемом режиме Greenfield, когда сеть 802.11n развернута и работает таким образом, что обратная совместимость с устаревшими устройствами 802.11a/b/g не требуется. Это наиболее эффективный режим сети 802.11n, поскольку он позволяет полностью использовать набор функций 802.11n. Если требуется защита устаревших устройств, нужно будет пожертвовать скоростью передачи данных как на уровне PHY, так и на уровне MAC стандарта 802.11n.

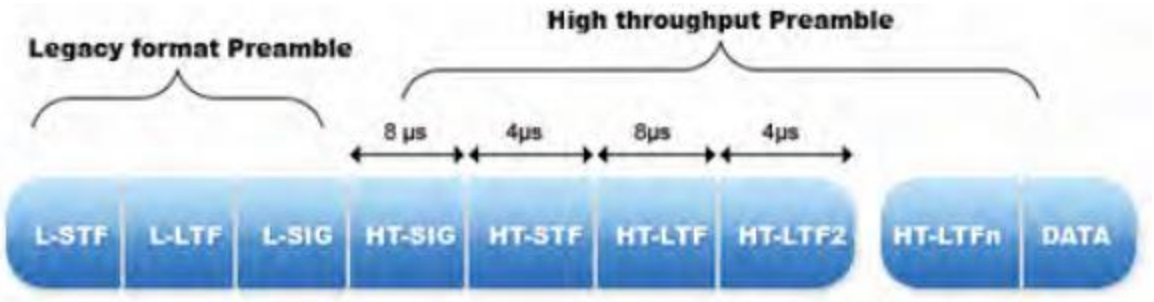
Однако в течение следующего года или около того наиболее распространенным режимом работы точки доступа 802.11n будет обязательный режим HT Mixed. В этом режиме улучшения режима HT могут использоваться одновременно с механизмами защиты HT, которые разрешают связь с устаревшими станциями. Смешанный режим HT (HT Mixed) обеспечивает обратную совместимость, но устройства 802.11n значительно теряют в пропускной способности по сравнению с режимом Greenfield.

На уровне PHY, когда необходима защита от устаревших устройств, устройства 802.11n должны передавать преамбулу смешанного режима даже при передаче HT (802.11n High Throughput). Преамбула смешанного режима по существу является преамбулой устаревшего формата, за которой следует преамбула HT. Это позволяет устаревшим станциям, которые не понимают преамбулу HT, по-прежнему распознавать передачу и откладывать использование среды. В развертывании Greenfield используется только преамбула HT:



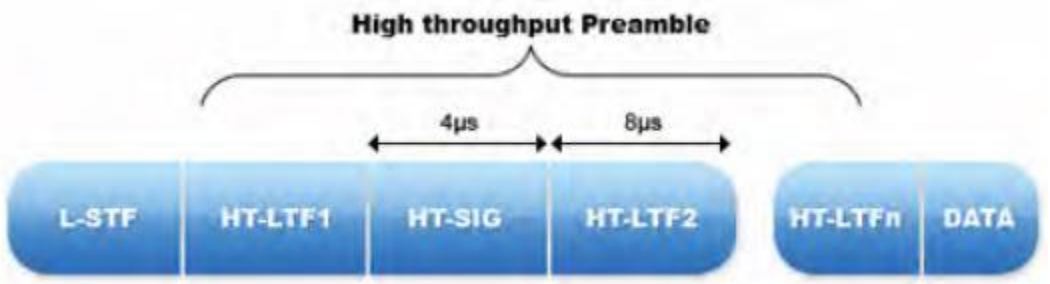
µs	мкс
Short training field	Короткое обучающее поле
Long training field	Длинное обучающее поле
Signal Field	Поле сигнала

Преамбула устаревшего формата



Legacy formal Preamble	Преамбула устаревшего формата
High throughput Preamble	Преамбула высокой пропускной способности
µs	мкс

Преамбула смешанного режима



High throughput Preamble	Преамбула высокой пропускной способности
µs	мкс

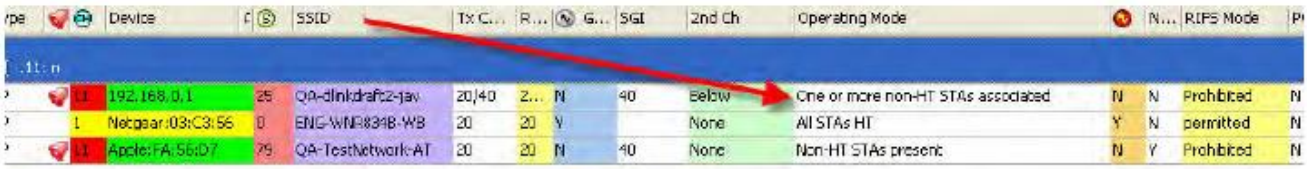
Преамбула режима HT

Еще на большие уступки приходится идти на уровне MAC, так как передачам 802.11n в режиме HT должны предшествовать низкоскоростные обмены кадрами устаревшего формата CTS-to-self, RTS/CTS или аналогичными, чтобы в устаревших узлах заработали механизмы контроля виртуальной несущей. Устаревшие узлы обновляют свой вектор распределения сети (NAV), который используется для виртуального определения того, когда среда снова станет свободной, на основе полей Duration/ID в этих кадрах. Это значит, когда требуется защита, передача в режиме HT (потенциально) использует больше времени для кадров «защиты», чем для собственных данных. Несмотря на то, что кадры типа RTS и CTS относительно короткие, для обмена кадрами RTS/CTS с устаревшей скоростью 6 Мбит/с потребуется больше времени, чем для передачи 500 байтов с максимальной скоростью передачи данных 802.11n.

Следует отметить, что для начала действия этих механизмов защиты устаревшая станция даже не должна быть связана с BSS 802.11n. Просто присутствие кадров от устаревших устройств заставляет сети 802.11n Greenfield понижать производительность до работы в смешанном режиме.

Решение AirMagnet

Приложение AirMagnet Wi-Fi Analyzer предупреждает о точке доступа с поддержкой HT (AirMagnet обнаруживает точку доступа, передающую трафик HT) и её рабочем канале, когда обнаруживает, что точка доступа указывает в сигнале маяка рабочий режим, равный 3 (одна или несколько подключенных станций non-HT), либо обнаруживает подключение станций non-HT к точке доступа, но не реализует какой-либо механизм защиты для защиты своей передачи от устаревших устройств.



Экран Easy View 802.11n приложения AirMagnet Wi-Fi Analyzer, показывающий точку доступа с поддержкой HT и связанные с ней станции, не поддерживающие HT

Пользователи приложения AirMagnet WiFi Analyzer могут получить эту информацию для точек доступа 802.11n, выбрав на экране Start опцию Easy View > View by 802.11n (Легкий просмотр > Просмотр по 802.11n).

Greenfield-Capable BSS Operating in Mixed Mode (BSS с поддержкой Greenfield, работающий в смешанном режиме)

Описание сигнала тревоги и возможные причины

Пользователи 802.11n имеют возможность работать в так называемом режиме Greenfield, когда сеть 802.11n развернута и работает таким образом, что обратная совместимость с устаревшими устройствами 802.11a/b/g не требуется. Это наиболее эффективный режим сети 802.11n, поскольку он позволяет полностью использовать набор функций 802.11n. Если требуется защита устаревших устройств, нужно будет пожертвовать скоростью передачи данных как на уровне PHY, так и на уровне MAC стандарта 802.11n.

Однако в течение следующего года или около того наиболее распространенным режимом работы точки доступа 802.11n будет обязательный режим HT Mixed. В этом режиме улучшения режима HT могут использоваться одновременно с механизмами защиты HT, которые разрешают связь с устаревшими станциями. Смешанный режим HT (HT Mixed) обеспечивает обратную совместимость, но устройства 802.11n значительно теряют в пропускной способности по сравнению с режимом Greenfield. Следует отметить, что устаревшая станция даже не должна быть связана с BSS 802.11n, чтобы эти механизмы защиты начали действовать. Простое присутствие кадров от устаревших устройств заставляет сети 802.11n Greenfield понижать производительность до смешанного режима.

Станции Clause 20 (далее именуемые станции HT) с помощью кадров маяка и ответа на зондирование передают информацию о том, станции какого типа наблюдаются. Эти кадры несут информационный элемент HT, который включает следующие поля:

- Operating Mode (Рабочий режим)
- Non-Greenfield STAs Present (Присутствуют станции, не поддерживающие Greenfield)
- OBSS Non-HT STAs Present (Присутствуют станции OBSS non-HT)

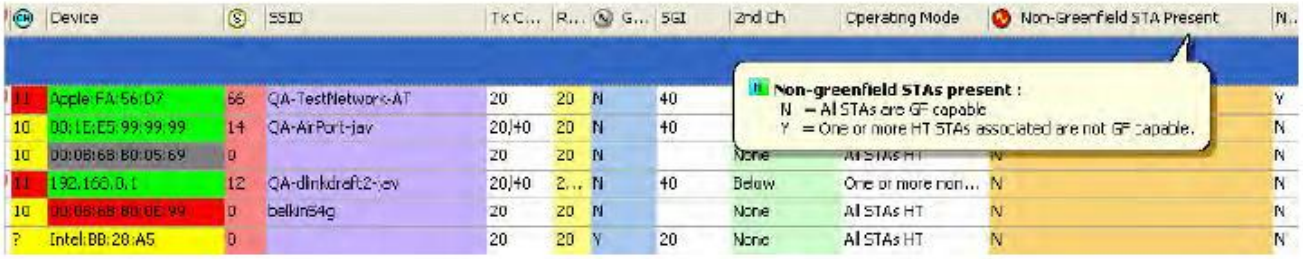
В поле Operation Mode показан рабочий режим BSS; оно может принимать одно из четырех возможных значений:

- 0: Все станции в BSS являются станциями HT (в BSS нет станций non-HT).
- 1: Станции non-HT присутствуют в первичном и/или вторичном канале.
- 2: Все станции в BSS являются станциями HT, однако, по крайней мере, одна станция поддерживает работу только на 20 МГц
- 3: В BSS присутствует одна или несколько станций non-HT.

Поле присутствия станций, не поддерживающих Greenfield, показывает, могут ли все подключенные станции HT поддерживать Greenfield.

Решение AirMagnet

Приложение AirMagnet Wi-Fi Analyzer предупреждает о точке доступа и ее рабочем канале, когда обнаруживает, что точка доступа указывает режим работы 3 (одна или несколько подключенных станций Non-HT), или использует один из механизмов защиты 802.11n, но все подключенные к ней станции поддерживают режим Greenfield или точка доступа сообщает об отсутствии подключенных станций non-GF. Для использования всех преимуществ режима высокой пропускной способности 802.11n AirMagnet рекомендует сделать так, чтобы все устройства с поддержкой Greenfield работали в режиме Greenfield.



На экране Easy View приложения AirMagnet WiFi Analyzer 802.11n отображаются устройства, совместимые с Greenfield

Diversity Insufficient for MIMO (Недостаточное разнесение для MIMO)

Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer обнаружило низкую пропускную способность MIMO, которая может быть связана с недостаточным разнесением передающей антенны (Tx Antenna) или путей передачи (Tx Path). Системы MIMO используют преимущества пространственного объединения (и потенциально пространственно-временных кодовых блоков) для увеличения пропускной способности. Подобное увеличение может снижаться, если пространственные сигнатуры каждого принимаемого потока недостаточно разнесены. Это может быть следствием влияния окружающей среды или пространственного разнесения передающих антенн.

Решение AirMagnet

Данные будут предоставлены позднее. Может не быть реализовано, в зависимости от дальнейшего тестирования и анализа.

Missing Performance Options (Отсутствуют параметры производительности)

Описание сигнала тревоги и возможные причины

Стандарт IEEE 802.11b определяет несколько дополнительных возможностей устройства, позволяющих повысить уровень его производительности:

- Короткая преамбула: Под преамбулой понимается информация заголовка в пакете. Как правило, более длительное время преамбулы просто дает устройству, декодирующему пакет, больше времени для работы. Более короткая преамбула обычно предназначена для повышения эффективности за счет уменьшения задержки во время процесса декодирования (это важно в системах, которые особенно чувствительны к задержкам, например, в тех, что реализуют передачу голоса по IP).
- Радиочастотная модуляция PBCC: PBCC (Packet Binary Convolutional Coding - двоичное пакетное сверточное кодирование) - это проприетарная настройка в некоторых устройствах, которая потенциально может увеличить скорость сети выше стандартного теоретического предела производительности 802.11b. Хотя это и может повысить производительность вашей сети, возможно, придется использовать точки доступа и карты доступа только определенного производителя.
- Гибкость канала (Channel agility): Этот параметр вашей точки доступа позволяет устройству во время первоначальной настройки искать наименее загруженный канал. Без этой функции устройство может использовать перегруженный канал, что приведет к помехам.

Решение AirMagnet

В процессе проектирования и развертывания WLAN можно воспользоваться этими дополнительными возможностями и положиться на них. Если вы включили данный сигнал тревоги, приложение AirMagnet WiFi Analyzer будет отслеживать эти возможности и подавать сигнал тревоги, если какие-либо беспроводные устройства не поддерживают данные опции.

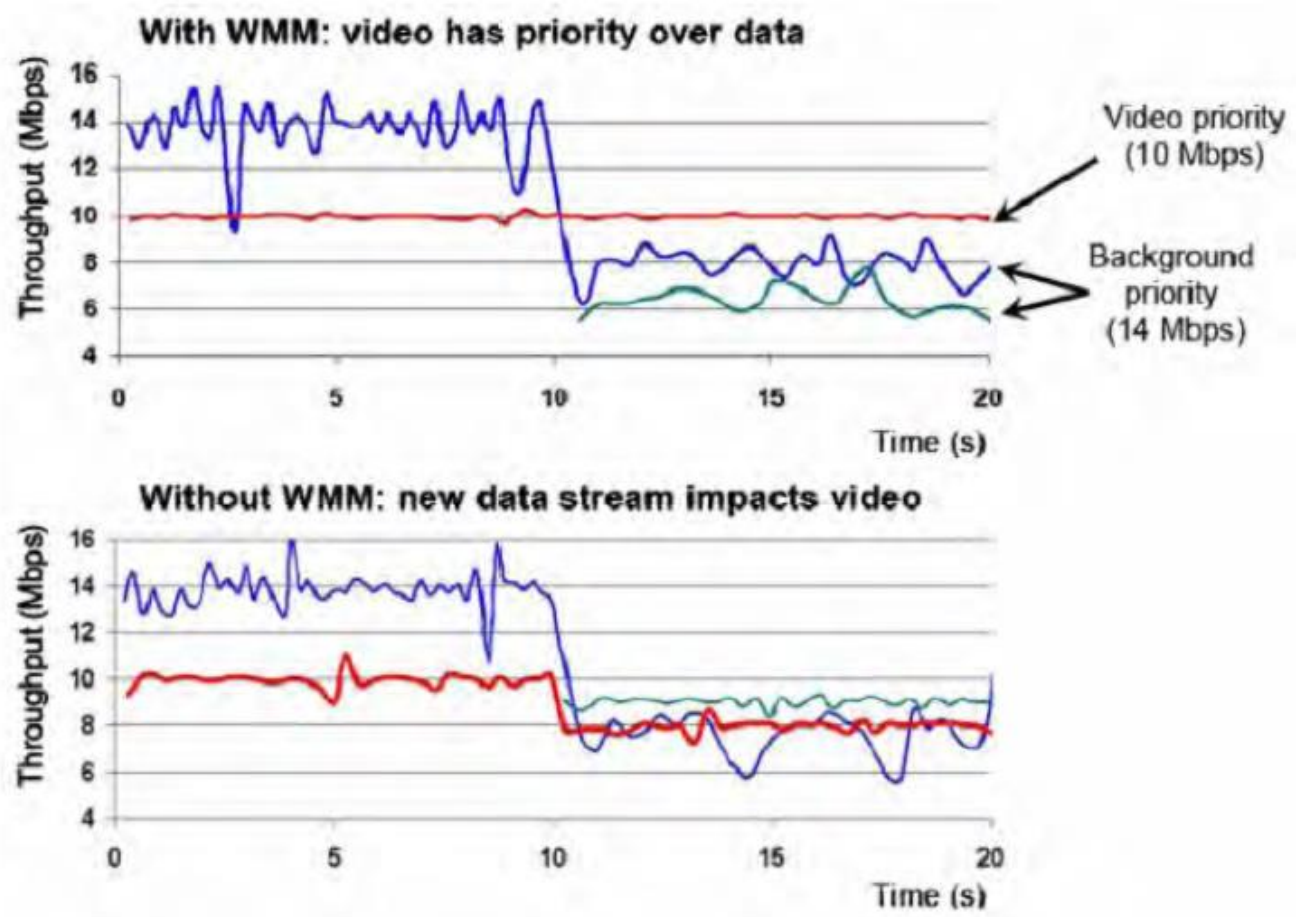
QoS Disabled on 802.11n AP (QoS отключено на точке доступа 802.11n)

Описание сигнала тревоги и возможные причины

Согласно стандарту 802.11, все пользователи сети WLAN используют пропускную способность сети совместно, и ни один пакет не имеет приоритета над любым другим пакетом. Обычно это не вызывает проблем при использовании типовых приложений обработки данных (например, электронной почты, сети Интернет, передачи файлов), но становится очень критичным в случае голосовых вызовов и потокового видео, когда пакеты должны проходить через сеть в нужное время, чтобы избежать прерываний или разъединений. QoS (Качество обслуживания) помогает гарантировать приоритет для определенных приложений. Если QoS не реализовано, и все пакеты имеют одинаковый приоритет, все пакеты, независимо от приложения (данные, голос, видео), будут иметь равные шансы быть отброшенными в случае перегрузки. Это очень важно для сетей 802.11n, где могут быть такие мультимедийные приложения, как видеопотоки высокой четкости, передаваемые одновременно с потоками голоса и данными.

Стандарт 802.11 был разработан с двумя коммуникационными методами: DCF (Distributed Coordination Function – распределенная функция координации) и PCF (Point Coordination function - функция координации точек). В режиме DCF, прежде чем станции смогут передавать данные или обнаруживать какие-либо коллизии, они должна убедиться, что среда передачи свободна. В режиме PCF точки доступа действуют как координаторы точек и периодически отправляют параметры станциям и опрашивают их на наличие данных. Ни один из этих методов не учитывает тип трафика или приоритет. Стандарт IEEE 802.11e вводит EDCF (Enhanced Distributed Coordination Function - расширенную распределенную функцию координации) и HCF (Hybrid Coordination Function - гибридную функцию координации).

В EDCF станции имеют разные уровни приоритета. Когда среда передачи свободна, станции ждут в течение периода времени, определенного соответствующим уровнем приоритета трафика, который называется AIFS (Arbitration Interframe Space – Арбитражное межкадровое пространство). Категория трафика с более высоким приоритетом будет иметь более короткое значение AIFS, чем категория трафика с более низким приоритетом. Таким образом, станции с трафиком более низкого приоритета выжидают дольше, чем станции с трафиком высокого приоритета, прежде чем попытаться получить доступ к среде. Кроме того, конфликтов можно избежать за счет использования перед передачей дополнительных временных интервалов, называемых окном конкуренции. Если станция обнаруживает, что другая станция передает данные, она должна дождаться следующего периода бездействия и продолжить обратный отсчет. Благодаря гибридной функции координации (HCF) гибридный контроллер будет в течение периода без конкуренции опрашивать станции и предоставлять станции конкретное время начала и максимальную продолжительность передачи.



With WMM: video has priority over data	С WMM: видео имеет приоритет перед данными
Throughput (Mbps)	Пропускная способность (Мбит/с)
Video priority (10 Mbps)	Приоритет видео (10 Мбит/с)
Background priority (14 Mbps)	Приоритет фона (14 Мбит/с)
Time (s)	Время (с)
Without WMM: new data stream impact video	Без WMM: новый поток данных влияет на видео

Эффекты от реализации QoS

Решение AirMagnet

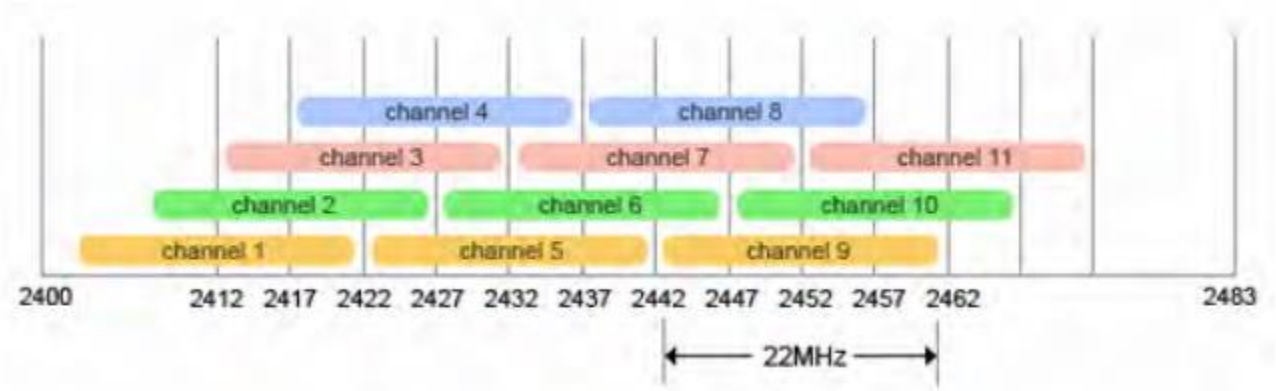
Приложение AirMagnet WiFi Analyzer способно обнаруживать точки доступа 802.11n, на которых не реализовано QoS, что может приводить к определенной задержке передачи трафика с более высоким приоритетом, например, голоса. Это может приводить к прерываниям звука или разъединению вызовов. Когда одной и той же точкой доступа обслуживаются разные типы трафика, AirMagnet рекомендует использовать на точке доступа функцию QoS, если она доступна.

40-MHz Channel Mode Detected in 2.4 GHz Spectrum (В частотном спектре 2,4 ГГц обнаружен режим канала 40 МГц)

Описание сигнала тревоги и возможные причины

Устаревшие системы 802.11 работают на каналах шириной 20 МГц (на самом деле каналы имеют ширину 22 МГц, но обычно их называют каналами 20 МГц). Стандарт 802.11n определяет работу канала шириной 20 и 40 МГц. При работе в режиме 40 МГц пропускная способность канала фактически вдвое больше, чем у устаревших систем. Это можно сравнить с «удвоением количества полос на автостраде, чтобы в два раза больше машин могло проехать».

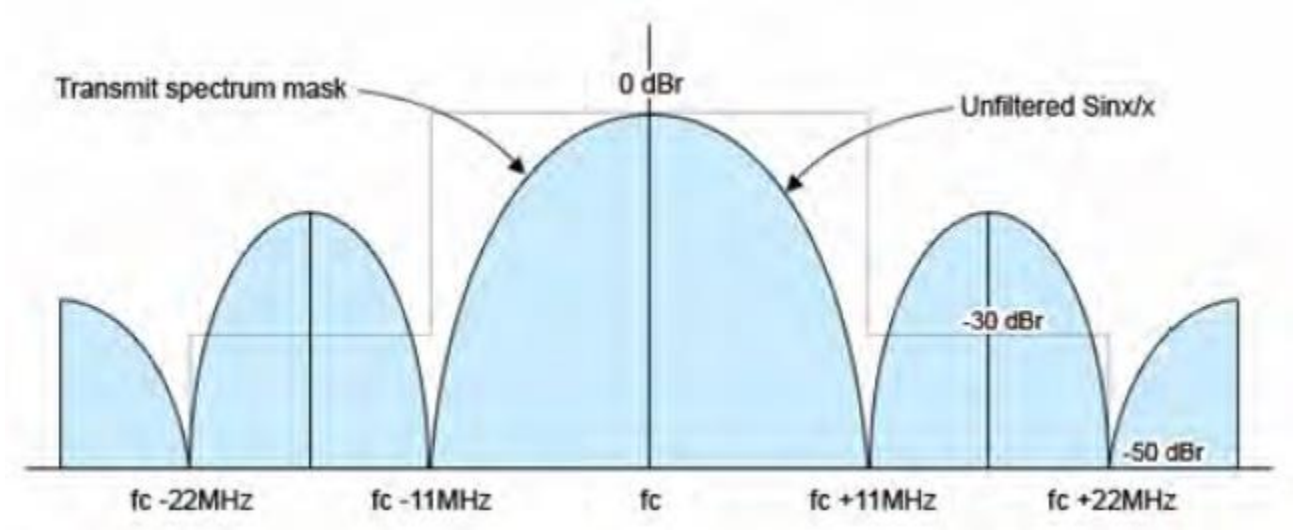
Четырнадцать каналов 802.11 в диапазоне 2,4 ГГц (в США используется одиннадцать каналов) расположены на расстоянии 5 МГц друг от друга с центральными частотами от 2412 МГц до 2477 МГц.



Channel	Канал
MHz	МГц

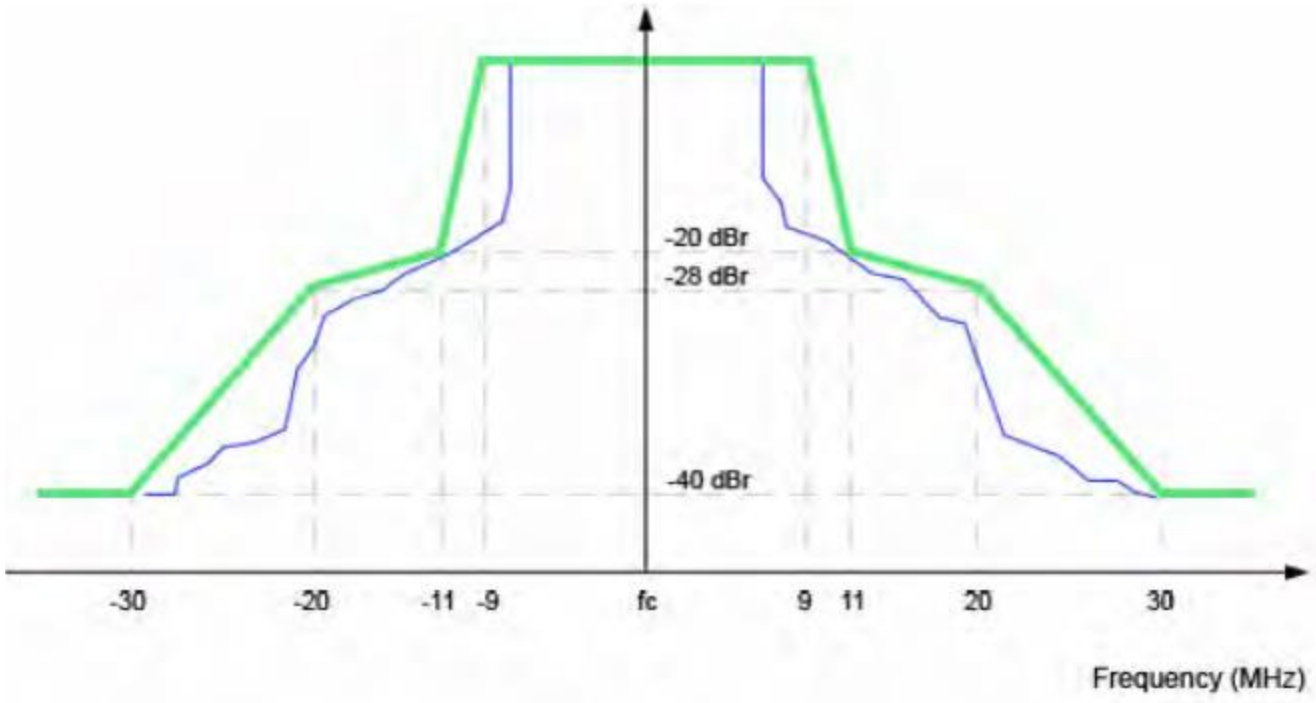
Схема формирования каналов в Северной Америке

Радиочастотные каналы не имеют четких границ. Модулированная часть (20 МГц) радиочастотного сигнала 802.11 «попадает» в +/- 11 МГц от центральной частоты (таким образом, ширина составляет 22 МГц); однако имеется некоторая «утечка» или немодулированная радиочастотная энергия, которая присутствует в диапазоне примерно до +/- 30 МГц от центральной частоты (при относительно гораздо более низких уровнях мощности). Количество радиочастотной энергии, присутствующей за пределами границы канала +/- 11 МГц, определяет спектральная маска.



Transmit spectrum mask	Маска спектра передачи
Unfiltered Sinx/x	Sinx/x без фильтрации
MHz	МГц
dBr	дБп

Спектральная маска 802.11b (DSSS/CCK)



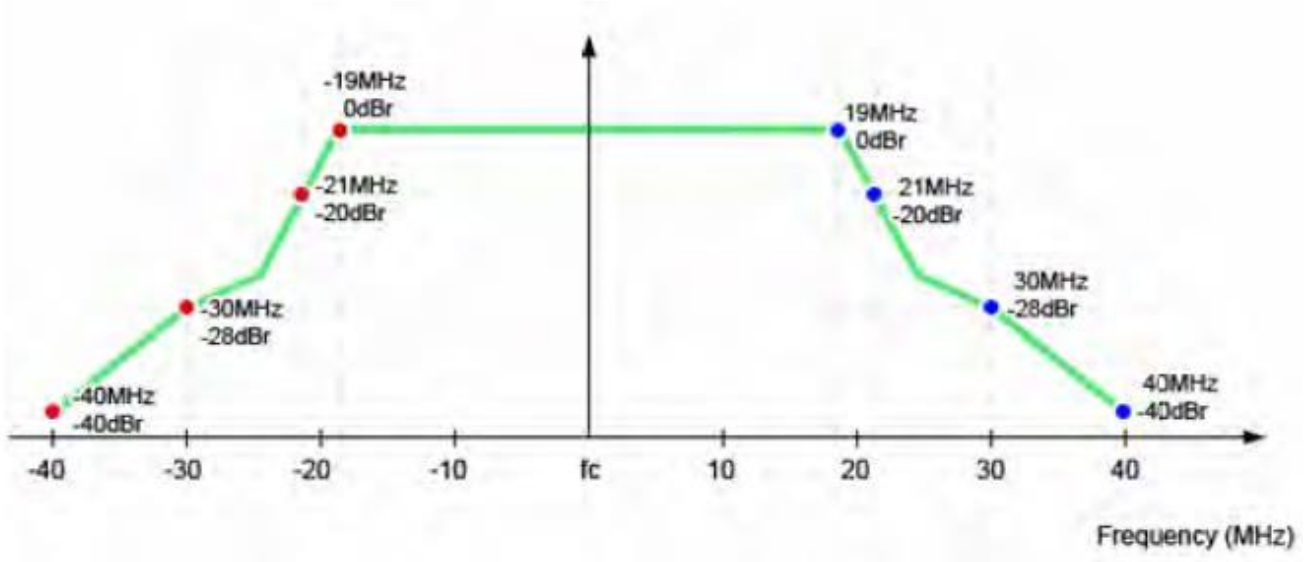
dBr	дБп
Frequency (MHz)	Частота (МГц)

Спектральная маска 802.11g (OFDM)

Таким образом, передача по стандарту 802.11 «занимает» 5 каналов (центральный, два смежных слева и два смежных справа). В зависимости от мощности передачи и чувствительности приемника передача может даже вызвать помехи на нескольких дополнительных каналах (до пяти каналов от центрального).

Например, устройство, ведущее передачу на канале 6, безусловно, вызовет значительные помехи на каналах 5 и 7 и некоторые помехи на каналах 4 и 8. Оно может даже вызвать помехи (обычно незначительные) на каналах 2, 3, 9 и 10. Именно поэтому в регионах, где регулирование ведется Федеральной комиссией связи США, в диапазоне 2,4 ГГц фактически имеется всего три одновременно используемых канала 802.11 шириной 20 МГц. Для борьбы с «утечкой» типовое развертывание сети

стандарта 802.11 b/g в Северной Америке предполагает использование точек доступа на каналах 1, 6 и 11. Такая схема развертывания каналов позволяет точкам доступа, находящимся в непосредственной близости друг от друга, минимизировать взаимные помехи.
Работа в режиме 40 МГц в частотном диапазоне 2,4 ГГц значительно усугубляет данную проблему. Как видно на следующем рисунке, спектральная маска 40 МГц обязательно приводит к тому, что на соседних каналах будет присутствовать сигнал с более высокой энергией.



MHz	МГц
dBr	дБп
Frequency (MHz)	Частота (МГц)

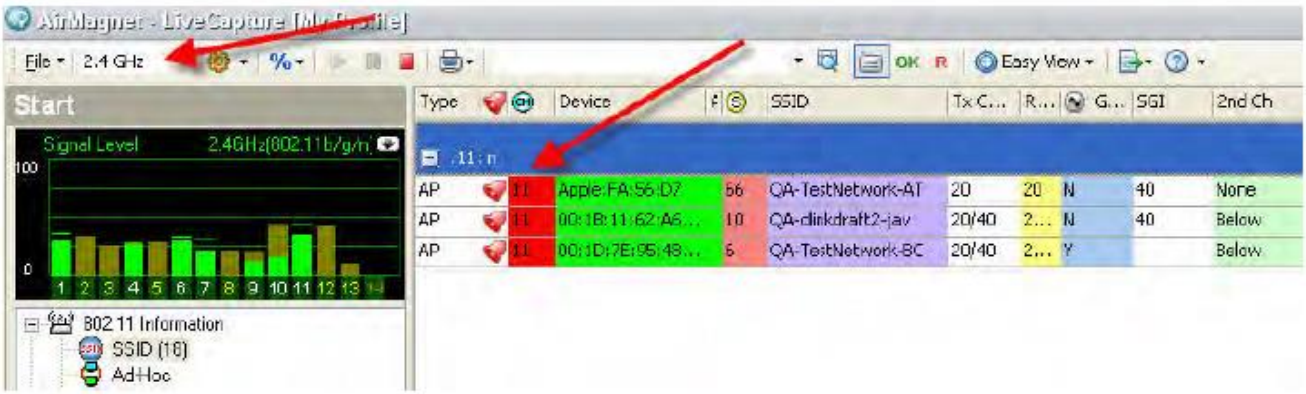
Спектральная маска 40 МГц

Таким образом, передача 802.11 по каналам 40 МГц в частотном диапазоне 2,4 ГГц занимает 9 каналов (центральный, четыре смежных слева и четыре смежных справа). Сразу очевидно, как передача 40 МГц в диапазоне 2,4 ГГц способна вызвать проблемы там, где есть только 11 используемых каналов. Решить эту проблему помогают механизмы сосуществования, но сложно разработать и развернуть эффективную многопользовательскую сеть, в которой для одной передачи может использоваться более 80% доступного спектра данного частотного диапазона.

Решение AirMagnet

Приложение AirMagnet Wi-Fi Analyzer предупреждает пользователей, когда обнаруживает точку доступа HT40 Upper или HT40 Lower, работающую в диапазоне 2,4 ГГц.

AirMagnet рекомендует использовать устройства стандарта 802.11n только в диапазоне 5 ГГц. В большинстве регуляторных доменов в диапазоне 5 ГГц существует гораздо больше доступных для использования каналов, а сами каналы разнесены на 20 МГц. Это обеспечивает гораздо больше «места» для работы канала шириной 40 МГц. Кроме того, следует отметить, что диапазон 2,4 ГГц намного более загружен, чем диапазон 5 ГГц, поскольку станции, работающие в диапазоне 2,4 ГГц, также должны бороться с устройствами Bluetooth, микроволновыми печами и другими распространенными источниками помех диапазона 2,4 ГГц, включая, например, и беспроводные телефоны.



Экран приложения AirMagnet WiFi Analyzer, на котором показаны точки доступа 802.11n, работающие в диапазоне 2,4 ГГц

HT-Enabled AP Ignoring Legacy Devices (Точка доступа с поддержкой HT игнорирует устаревшие устройства)

Описание сигнала тревоги и возможные причины

Этот сигнал тревоги следует логике, очень похожей на # 164 и # 167, за исключением того, что в поиск включается весь канал (а не только BSS).

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает точку доступа с поддержкой HT, которая либо не обнаруживает, либо игнорирует наличие устаревших устройств. В этом случае протоколы защиты могут не сработать, что приведет к блокировке устаревших устройств.

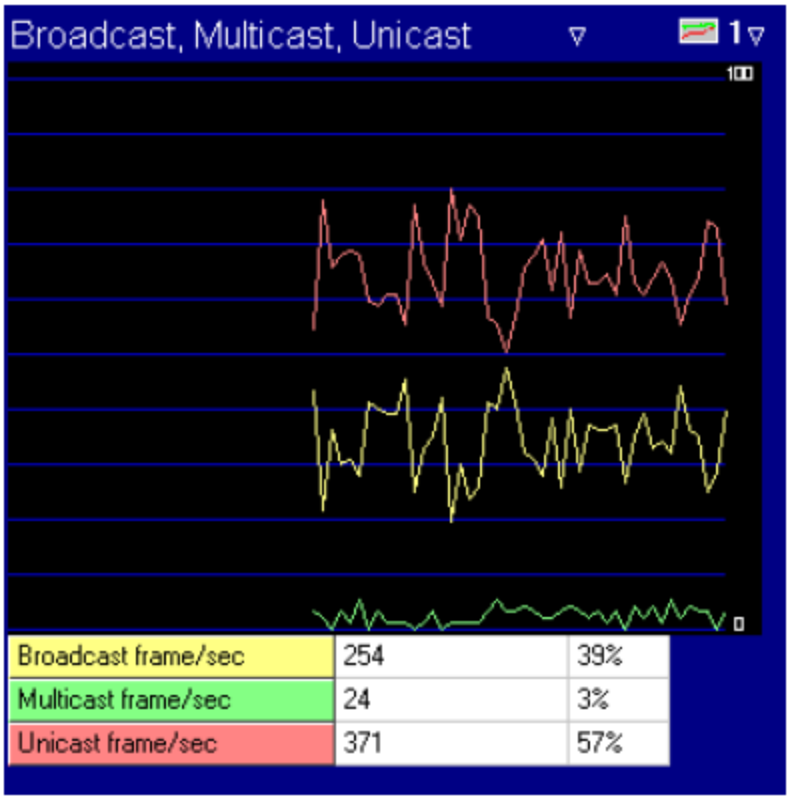
Excessive Multicast/Broadcast on Node (Чрезмерная многоадресная/широковещательная передача на узле)

Описание сигнала тревоги и возможные причины

Как и в проводной сети, чрезмерное количество широковещательных и многоадресных кадров создает дополнительную нагрузку на все устройства в проводной локальной сети. Более чувствительной к многоадресным и широковещательным кадрам по сравнению с проводными сетями сеть WLAN делает тот факт, что все многоадресные и широковещательные кадры передаются с низкой скоростью (например, 1 или 2 Мбит/с для WLAN 802.11b). Такие низкоскоростные передачи потребляют большую полосу пропускания сети WLAN.
Помимо неэффективного использования полосы пропускания низкоскоростные многоадресные и широковещательные кадры требуют большего времени для выполнения процесса передачи, что приводит к более высоким задержкам для других устройств, ожидающих освобождения беспроводной среды. Чрезмерное количество многоадресных и широковещательных кадров вызывает джиттер в таких чувствительных к задержке приложениях WLAN, как VoIP. Например, передача 1000-байтового кадра широковещательной передачи со скоростью 1 Мбит/с займет не менее 8 миллисекунд, что является значительной задержкой для голосового приложения.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает использование многоадресных и широковещательных кадров для каждого канала и устройства, чтобы сообщить о злоупотреблениях. Порог срабатывания сигнализации - это процентное отношение многоадресных и широковещательных кадров к общему количеству кадров по устройству или каналу. Для дальнейшего изучения ситуации с многоадресной и широковещательной рассылкой можно использовать показанный ниже экран Channel (Канал) или Infrastructure (Инфраструктура) приложения AirMagnet WiFi Analyzer, на котором отображается соответствующая статистика. (Просмотр экрана Channel (Канал) или Infrastructure (Инфраструктура) доступен через удаленный анализатор (Remote Analyzer) системы Enterprise, а также на ноутбуке или портативном анализаторе).

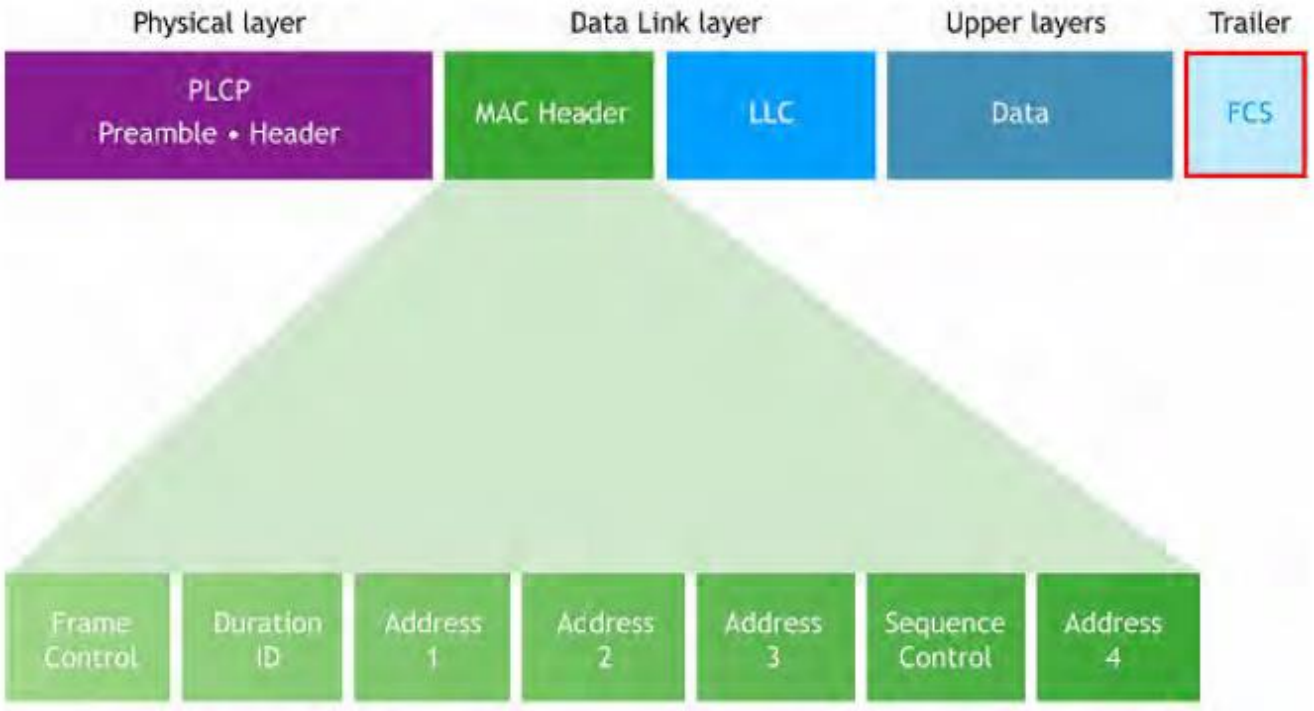


Кадры многоадресной и широковещательной передачи для возникновения сигнала тревоги о неправильном использовании

Excessive Frame Errors on Node (Чрезмерное количество кадровых ошибок на узле)

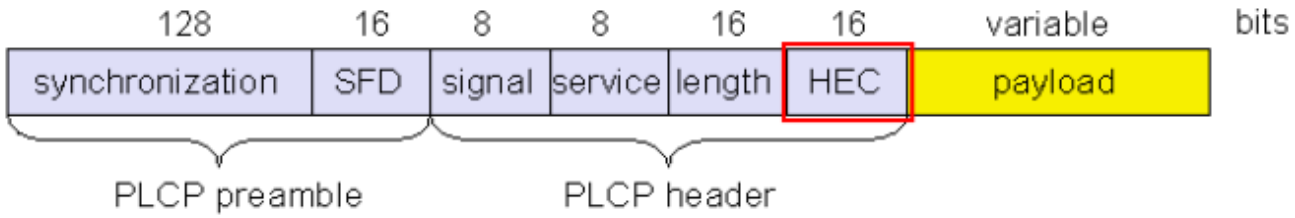
Описание сигнала тревоги и возможные причины

Радиочастотный спектр сети WLAN является открытым, динамическим, совместно используемым, подверженным шумам, помехам, коллизиям пакетов, многолучевому распространению, синдрому скрытых узлов и т.д. IEEE 802.11 имеет встроенный механизм проверки ошибок, позволяющий обнаруживать ошибки передачи и приема, вызванные любой из вышеупомянутых проблем. Например, спецификация физического уровня IEEE 802.11b DSSS (Direct Sequence Spread Spectrum – Расширение спектра по методу прямой последовательности) включает в заголовок PLCP (Physical Layer Convergence Protocol – Протокол сходимости физического уровня) поле HEC (Header Error Check - Проверка ошибок заголовка) для обнаружения ошибок (смотрите рисунок ниже). Приемник выполняет вычисления в полях синхронизации, обслуживания и длины и сравнивает их с переданным значением. Если результаты не совпадают, получатель должен принять решение об аварийном завершении кадра.



Physical layer	Физический уровень
Data link layer	Уровень канала передачи данных
Upper layers	Верхние уровни
Trailer	Концевик
Preamble – Header	Преамбула – Заголовок
MAC Header	Заголовок MAC
Data	Данные
Frame Control	Управление кадром
Duration ID	Идентификатор продолжительности
Address	Адрес
Sequence Control	Управление последовательностью

Кадр IEEE 802.11 включает контрольную сумму в PLCP и FCS для заголовка кадра и тела кадра соответственно



Synchronization	Синхронизация
Signal	Сигнал
Service	Служба
Length	Длина
Variable bits	Переменное количество битов
Payload	Полезная нагрузка
PLCP preamble	Преамбула PLCP
PLCP header	Заголовок PLCP

HEC (Контрольная сумма ошибки заголовка), заданная в заголовке PLCP

Протокол уровня MAC 802.11 для обнаружения ошибок также задает поле FCS (Frame Checksum - Контрольная сумма кадра) в конце пакета. Смотрите рисунок ниже.

Frame Control	Duration ID	Address1 (source)	Address2 (destination)	Address3 (rx node)	Sequence Control	Address4 (tx node)	Data	FCS
2	2	6	6	6	2	6	0 - 2,312	4

Управление кадром	Идентификатор продолжительности	Адрес 1 (источник)	Адрес 2 (адресат)	Адрес 3 (узел приема)	Последовательное управление	Адрес 4 (узел передачи)	Данные	FCS
2	2	6	6	6	2	6	0 – 2312	4

FCS (Контрольная сумма кадра), задаваемая в формате протокола MAC 802.11

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает эти кадры с ошибками и отслеживает их в зависимости от устройства и ориентации канала. Смотрите рисунок ниже:

Speed		
Alert	0	
Frames/Bytes	997	90645
Retry frames	19	1 %
Ctrl. frames	464	46 %
Mgmt. frames	50	5 %
Data frames	343	34 %
CRC frames	140	14 %
Ctrl. Bytes	15812	17 %
Mgmt. Bytes	4657	5 %
Data Bytes	50646	55 %
CRC error Bytes	19530	21 %
Ctrl. Frames/Bytes	464	15812
Mgmt. Frames/Bytes	50	4657
Data Frames/Bytes	343	50646

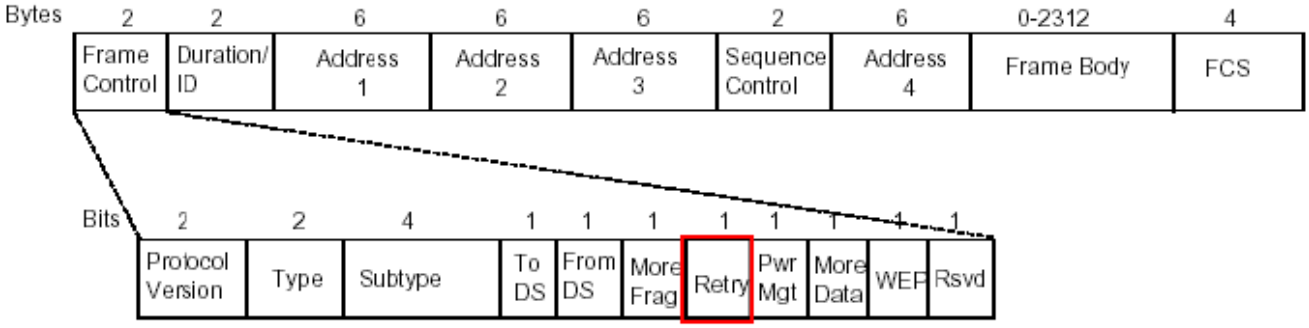
Отображение отслеживания ошибок кадра CRC приложением AirMagnet WiFi Analyzer для канала или устройства

Когда отношение кадров с ошибкой CRC к общему количеству кадров превышает определяемое пользователем пороговое значение, приложение AirMagnet WiFi Analyzer предупреждает администратора о возможных проблемах с производительностью сети WLAN.

Excessive Frame Retries on Node (Чрезмерное количество повторных попыток передачи кадра на узле)

Описание сигнала тревоги и возможные причины

Радиочастотный спектр сети WLAN является открытым, динамическим, совместно используемым, подверженным шумам, помехам, коллизиям пакетов, многолучевому распространению, синдрому скрытых узлов и т.д. При появлении ошибок, вызванных любой из вышеперечисленных проблем, передатчик кадра с ошибкой не получит кадр управления 802.11, называемый кадром подтверждения. При отсутствии подтверждения передатчик предполагает, что приемник не принял кадр успешно, и повторно передает неподтвержденный кадр с битом повтора (Retry) в кадре, установленным на единицу. Это указывает на повторную передачу. На рисунке ниже показано поле Retry в заголовке кадра 802.11.

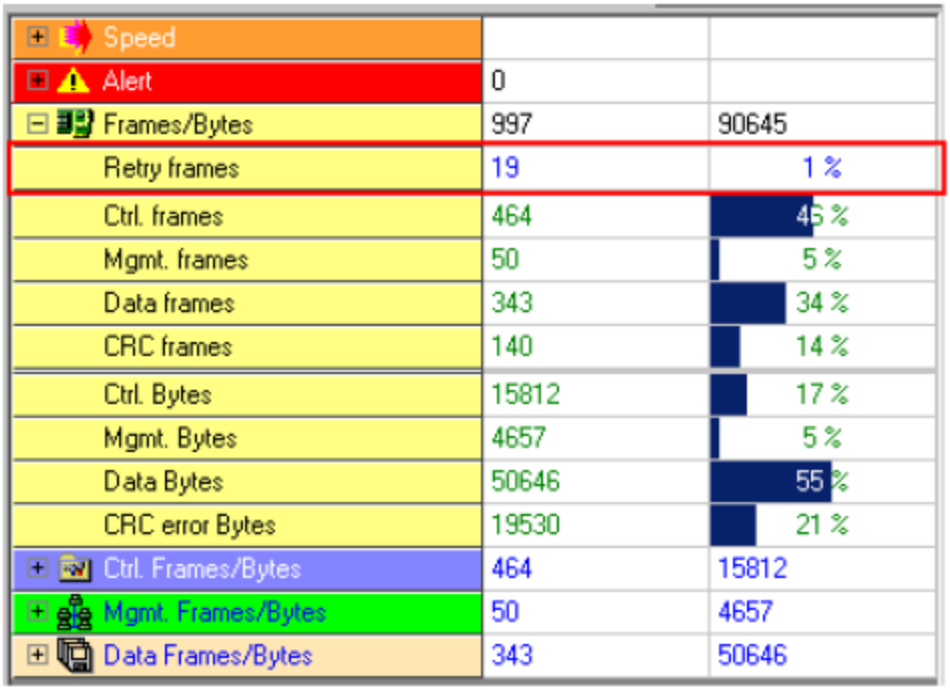


Bytes	Байты
Frame Control	Управление кадром
Duration/ID	Идентификатор/продолжительность
Address	Адрес
Sequence Control	Управление последовательностью
Frame Body	Тело кадра
Bits	Биты
Protocol Version	Версия протокола
Type	Тип
Subtype	Подтип
To DS	К DS
From DS	От DS
More Fragm	Большая фрагментация
Retry	Повторная попытка
Pwr Mgt	Управление мощностью
More Data	Больше данных
Rsvd	Зарезервировано

Заголовок кадра 802.11, включающий поле Retry для индикации повторной передачи кадра

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает кадры повтора и отслеживает их для каждого устройства и ориентации канала. Смотрите рисунок ниже:



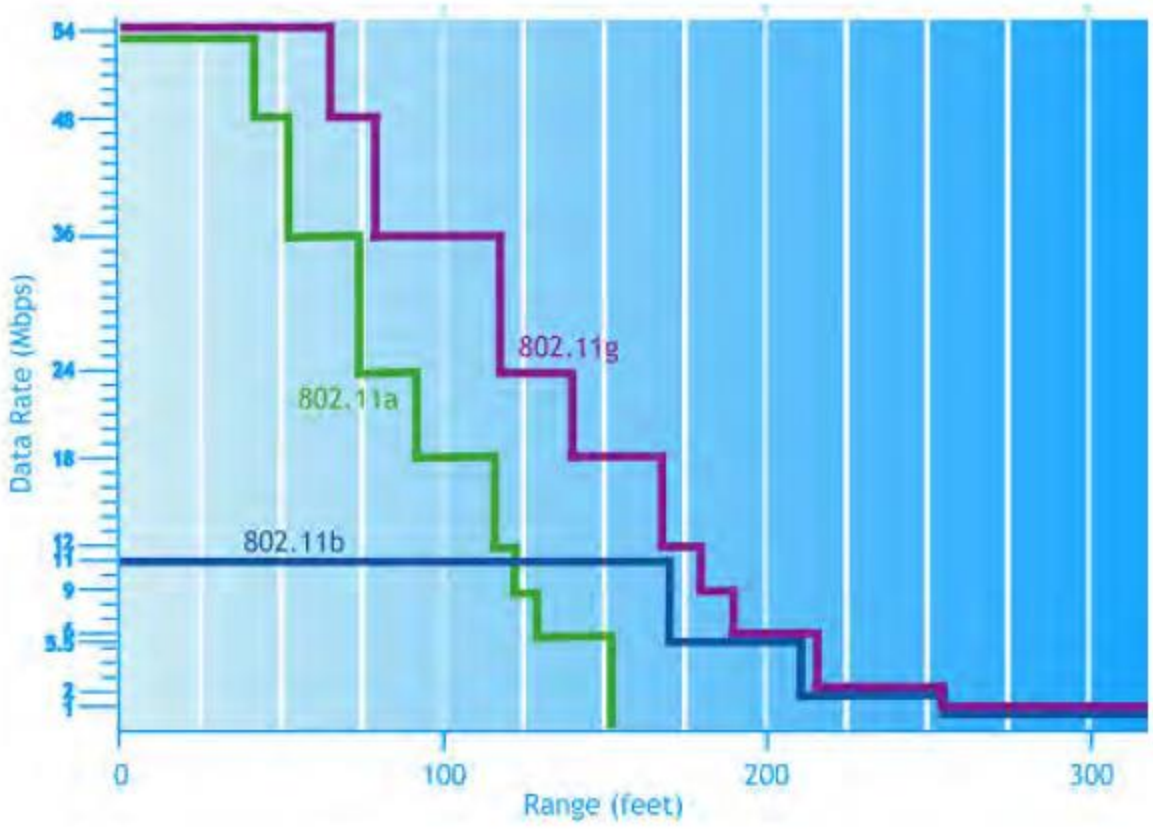
Отображение приложением AirMagnet WiFi Analyzer отслеживания кадров с ошибкой Retry (повторная попытка) для канала или устройства

Когда отношение количество повторных попыток передачи кадров к общему количеству кадров превышает заданное пользователем пороговое значение, приложение AirMagnet WiFi Analyzer предупреждает администратора о возможной проблеме производительности WLAN из-за шумов, помех, коллизий пакетов, многолучевого распространения, синдрома скрытого узла и т.д. После этого администратор получает возможность предпринять соответствующие шаги, чтобы избежать подобных проблем.

Excessive Low Speed Transmission on Node (Чрезмерно низкая скорость передачи на узле)

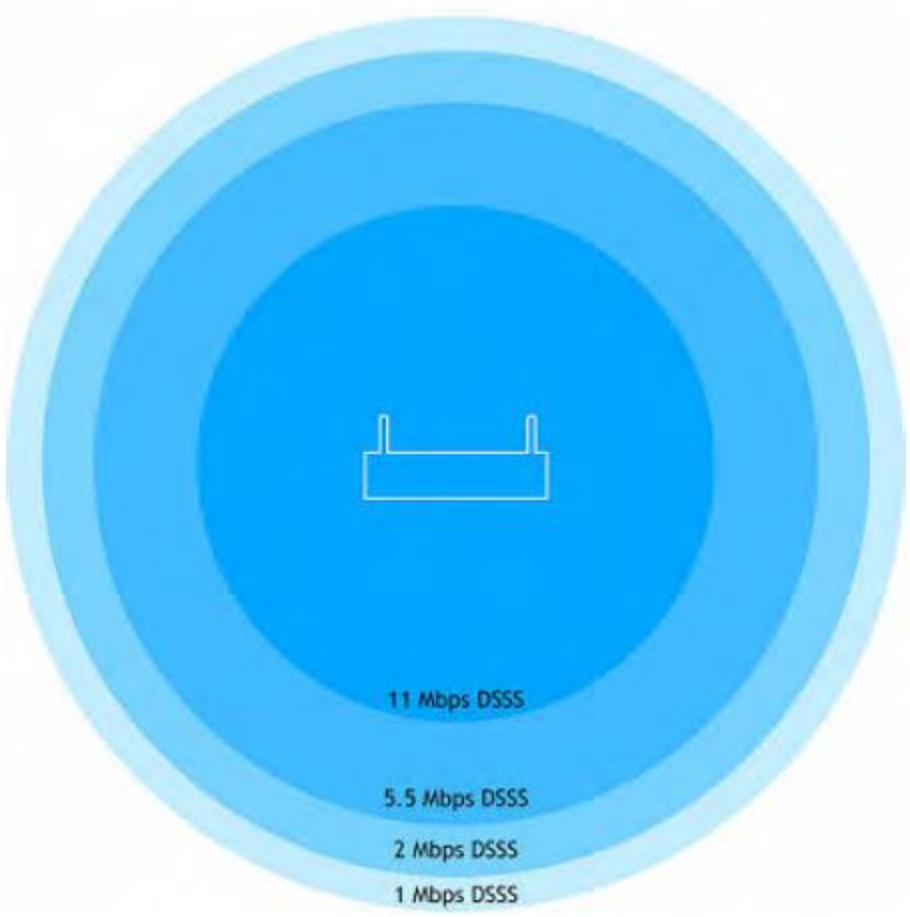
Описание сигнала тревоги и возможные причины

Устройства стандартов 802.11a, 11b или 11g от кадра к кадру используют несколько различных скоростей передачи. Более высокая скорость передачи требует меньшей полосы пропускания и обеспечивает более высокую пропускную способность. Оптимизация скорости передачи является ключевым фактором в процессе обследования площадки и развертывания сети WLAN. Обычно это зависит от качества сигнала и расстояния.



Data Rate (Mbps)	Скорость передачи данных (Мбит/с)
Range (feet)	Расстояние (футы)

Корреляция скорости и расстояния для 802.11 a/b/g



Mbps	Мбит/с

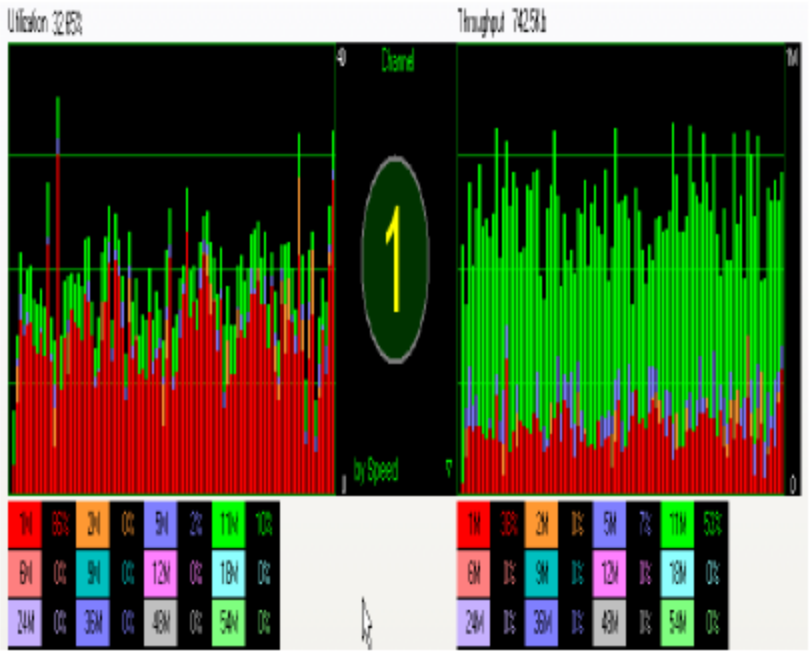
Корреляция скорости и покрытия 802.11b

В таблице ниже указаны все поддерживаемые скорости и то, что приложение AirMagnet WiFi Analyzer считает низкой скоростью для выбранного стандарта.

Скорость	802.11b (Мбит/с)	802.11g (Мбит/с)	802.11a (Мбит/с)
Поддерживаемая скорость	1, 2, 5.5, 11	1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48, 54	6, 9, 12, 24, 36, 48, 54
AirMagnet Wi-Fi считает низкой скоростью	1, 2	1, 2, 5.5, 6, 9, 11, 12, 24, 36	6, 9, 12, 24, 36

Поддерживаемые скорости передачи и те из них, которые приложение Wi-Fi AirMagnet Analyzer считает «низкой» скоростью

Однако для достижения такого же низкого уровня ошибок по сравнению с низкоскоростной передачей высокоскоростная передача требует более высокого качества сигнала. Выбор скорости передачи – это решение, принимаемое передатчиком, который также обнаруживает проблемы приема из-за отсутствия подтверждений. Передатчик может изменять скорость передачи для повышения надежности. Если этот сценарий применяется слишком часто, сеть WLAN замедляется и ее пропускная способность ухудшается. Обратите внимание на проблему, показанную на скриншоте экрана приложения AirMagnet WiFi Analyzer ниже. Там показана чрезмерно низкая скорость передачи (1 Мбит/с), высокая степень использования (32%) и низкая пропускная способность (931 Кбит/с).



Скриншот экрана приложения AirMagnet WiFi Analyzer, показывающий взаимосвязь использования полосы пропускания (Bandwidth Utilization), пропускной способности (Throughput) и скорости передачи (Transmit Speed)

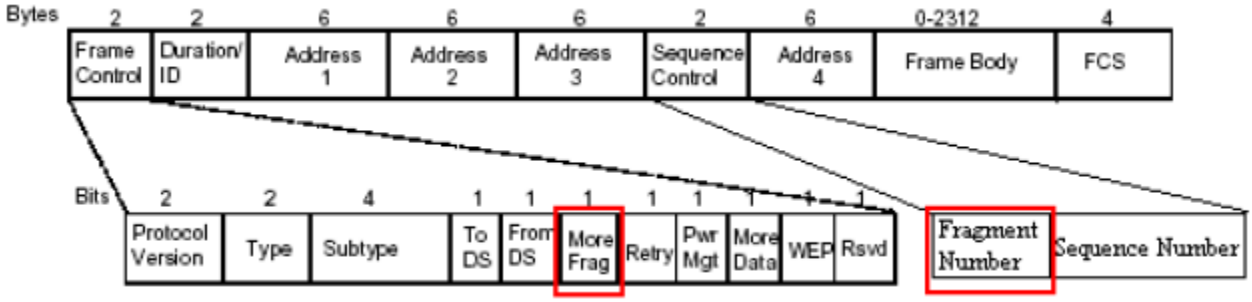
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer предупредит администратора, если увидит большой объем трафика на более низких скоростях, что может привести к чрезмерному использованию полосы пропускания и снижению пропускной способности. Администратор должен предпринять соответствующие шаги, чтобы повысить качество сигнала для получения более высоких скоростей передачи. Также важно отметить, что для избежания снижения скорости передачи расстояние от станций до точки доступа должно быть подходящим.

Excessive Fragmentation on Node (Чрезмерная фрагментация на узле)

Описание сигнала тревоги и возможные причины

Уровень MAC стандарта 802.11 поддерживает процессы фрагментации и дефрагментации. Процесс разделения кадра 802.11 на более мелкие кадры для последующей передачи называется фрагментацией. Этот процесс помогает повысить надежность и снизить количество ошибок. В случаях, когда характеристики канала ограничивают доступность приема, передача меньшими (фрагментированными) кадрами увеличивает вероятность успешной передачи. Фрагментация выполняется на каждом передатчике непосредственно перед фактическим началом передачи. Процесс рекомбинации фрагментированных кадров в исходный нефрагментированный более длинный кадр называется дефрагментацией. Стандарт IEEE 802.11 определяет формат пакета для идентификации фрагментированных кадров для дефрагментации (показано на рисунке ниже).



Bytes	Байты
Frame Control	Управление кадром
Duration/ID	Идентификатор/продолжительность
Address	Адрес
Sequence Control	Управление последовательностью
Frame Body	Тело кадра
Bits	Биты
Protocol Version	Версия протокола
Type	Тип
Subtype	Подтип
To DS	К DS
From DS	От DS
More Fragm	Большая фрагментация
Retry	Повторная попытка
Pwr Mgt	Управление мощностью
More Data	Больше данных
Rsvd	Зарезервировано
Fragment Number	Номер фрагмента
Sequence Number	Порядковый номер

Поля кадра IEEE 802.11 для фрагментации и дефрагментации кадра

Повышенная надежность фрагментированных кадров меньшего размера достигается за счет служебных данных передачи кадров. Кадр делится на разные сегменты в зависимости от порога фрагментации. Размещение фрагментов в процессе фрагментации определяется «полем управления последовательностью», как показано на рисунке выше. Поле «еще» указывает, является ли фрагмент последним.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает статистику фрагментации в сети и предупреждает о злоупотреблении фрагментацией, которое может привести к снижению производительности сети WLAN. Необходимо тщательно установить порог фрагментации, чтобы сбалансировать получаемую выгоду и служебные данные. Обычно поставщики оборудования устанавливают порог фрагментации по умолчанию равным 1536.

Identical Send and Receive Address (Одинаковый адрес отправки и получения)

Описание сигнала тревоги и возможные причины

Все передаваемые в беспроводной среде стандартные кадры 802.11 содержат несколько базовых структур, которые содержат передаваемые данные. Эти структуры могут различаться в зависимости от типа рассматриваемого кадра, но все типы кадров будут иметь как минимум два базовых компонента:

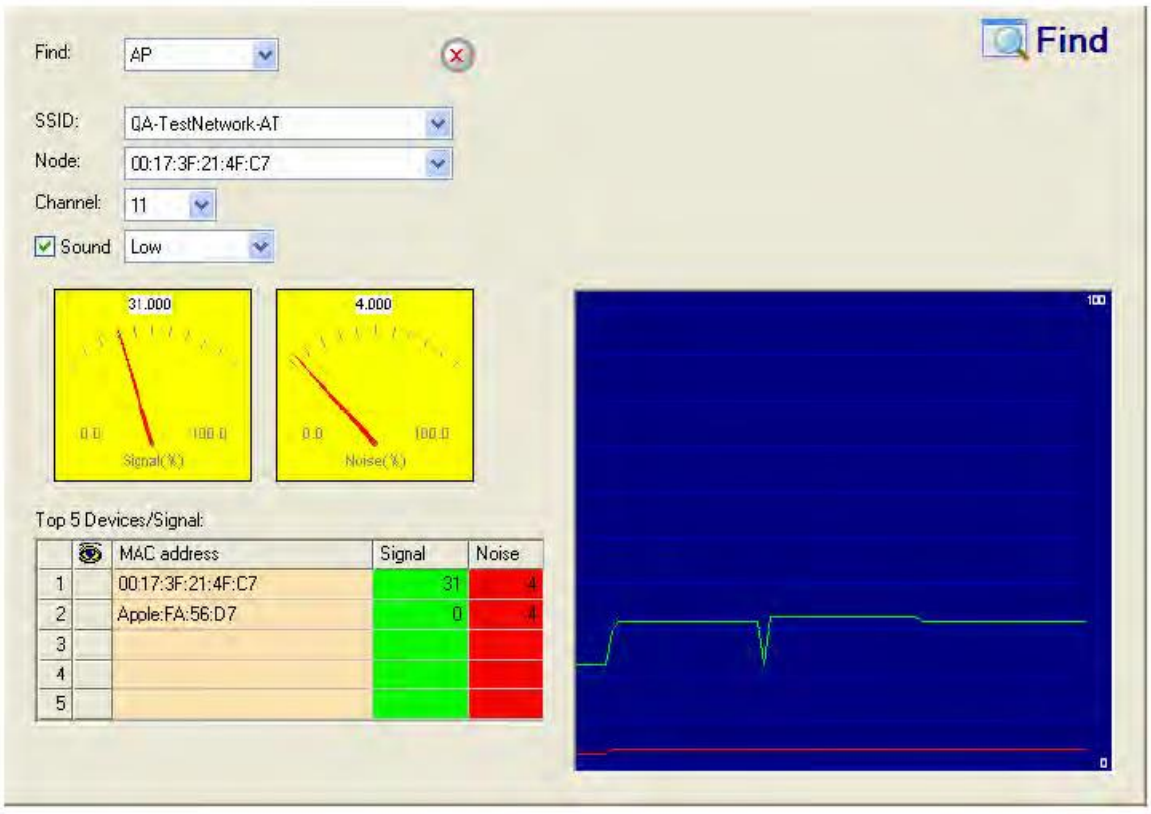
- Заголовок - Заголовок кадра содержит основную информацию об устройстве, которое первоначально передало кадр (например, «отправитель»), а также об устройстве, на которое следует отправить кадр (например, «получатель»).
- Полезная нагрузка - Полезная нагрузка кадра содержит большую часть фактических данных, передаваемых в кадре.

Чтобы подавить беспроводную активность в корпоративной сети, злоумышленники часто модифицируют беспроводные кадры для имитации характеристик тех кадров, что передаются легитимным пользователем. Подобные модификации могут включать изменения MAC-информации об отправителе и получателе кадров. Как правило, беспроводной трафик всегда будет включать как достоверный MAC-адрес отправителя (устройства, передавшего пакет), так и достоверный MAC-адрес получателя (предполагаемого получателя пакета). Поскольку устройству никогда не нужно отправлять пакеты самому себе, эти поля всегда должны содержать разные данные.

Для имитации корпоративного пользователя злоумышленники могут создавать кадры, которые кажутся передаваемыми с допустимого устройства, но в которых поля данных отправителя и получателя идентичны. Это может вызвать увеличение общего беспроводного трафика и потенциально способно привести к снижению пропускной способности сети для реальных пользователей.

Решение AirMagnet

В обычной сетевой среде отправитель и получатель кадра никогда не будут одинаковыми. Следовательно, при обнаружении таких моделей трафика приложение AirMagnet WiFi Analyzer подаст сигнал тревоги, чтобы предупредить ИТ-персонал о ненормальной работе сети. Администраторам рекомендуется использовать инструмент Find для нахождения проблемного устройства и его отключения или иного удаления из корпоративной среды.



Improper Broadcast Frames (Неправильные широковещательные кадры)

Описание сигнала тревоги и возможные причины

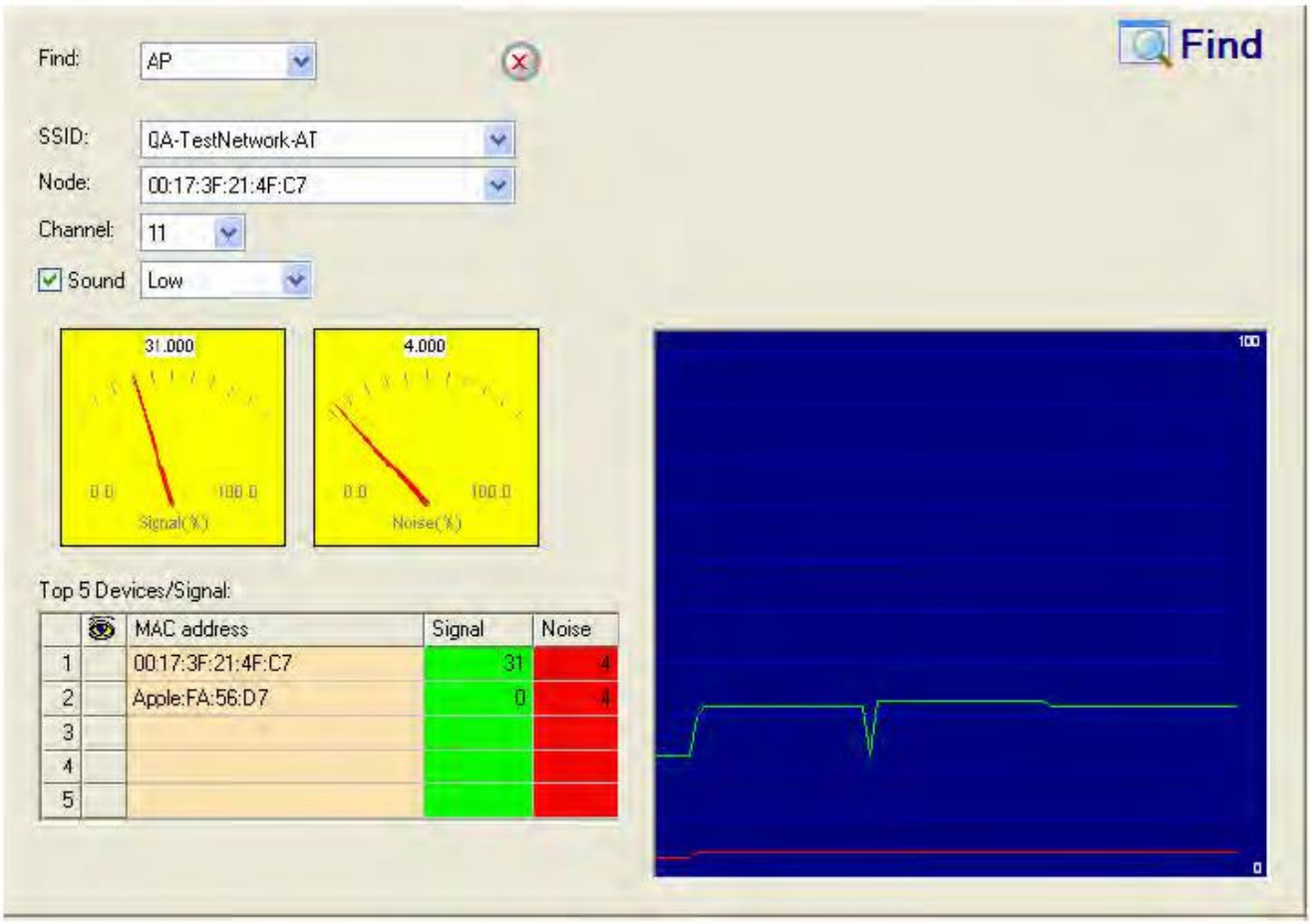
Вся связь в сетях 802.11 осуществляется с помощью передачи беспроводных «кадров», которые содержат необходимые данные. Когда беспроводные устройства передают эти кадры, они отправляются с помощью одного из трех механизмов:

- Широковещательная передача (Broadcast) - Кадры, которые передаются на все устройства в беспроводной среде, называются «широковещательными кадрами». Эти кадры обычно не предназначены для одного конкретного устройства. Примером широковещательного кадра являются сигналы маяка точки доступа.
- Многоадресная передача (Multicast) - Кадры, которые передаются группе из нескольких устройств, называются «многоадресными кадрами». Этот механизм позволяет точке доступа отправлять один и тот же кадр на несколько устройств одновременно, что способно помочь снизить использование сети. Практически любой кадр данных может быть передан через многоадресную рассылку; распространенными примерами являются кадры потоковой мультимедийной передачи.
- Одноадресная передача (Unicast) - Кадры, предназначенные для одного получателя, называются «одноадресными кадрами». В этих передачах определяющий получателя адрес назначения предоставляется в информации о кадре. Примером одноадресного кадра является кадр подтверждения ACK, передаваемый от точки доступа на станцию.

Стандартные развертывания 802.11 допускают некоторую гибкость в выборе механизмов передачи различных типов кадров. Однако если большое количество кадров передается через широковещательную или многоадресную передачу, это может снизить скорость передачи по сети и создать ненужный шум в беспроводной среде. Например, когда пользователь пытается установить беспроводное соединение, от станции на точку доступа передается кадр запроса подключения (Association Request). Этот кадр никогда не должен передаваться через широковещательную рассылку, так как он должен отправляться только на предполагаемую точку доступа. Передача подобного кадра в виде широковещательной рассылки только заставит другие устройства в сети сканировать передачу для определения того, являются ли они предполагаемыми получателями.
Злоумышленник может воспользоваться механизмом широковещательной рассылки, заполнив беспроводную среду ненужными широковещательными кадрами, что способно помешать другим пользователям получать данные или проводить стандартные беспроводные операции. Кроме того, из-за увеличения трафика может быть снижена скорость работы беспроводной сети.

Решение AirMagnet

Хотя сигнал тревоги о неправильных широковещательных кадрах может указывать на потенциальную атаку, часто он может быть результатом неправильно настроенной точки доступа или беспроводного клиента. В любом случае источник недопустимых кадров должен быть обнаружен с помощью инструмента Find (Найти).



После определения проблемного устройства обратитесь к ИТ-персоналу для его перенастройки в соответствии с корпоративной политикой беспроводной связи. После завершения этого процесса устройство должно работать нормально.

Simultaneous PCF and DCF Operation (Одновременная работа функций PCF и DCF)

Описание сигнала тревоги и возможные причины

Стандарт IEEE 802.11 определяет два протокола доступа к среде:

- PCF (Point Coordination function) – Функция координации точек, при которой точка доступа обычно действует как центральный координатор управления правом передачи по протоколу опроса. Все беспроводные клиентские станции по своей сути подчиняются правилам доступа к среде, установленным центральным координатором.
- DCF (Distributed Coordination Function) – Распределенная функция координации обеспечивает автоматическое совместное использование среды передачи с помощью CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance – Многостанционный доступ с контролем несущей и недопущением конфликтов) и случайного времени отсрочки передачи после состояния занятости среды. Кроме того, для всего направленного трафика используется немедленное положительное подтверждение (кадр ACK), когда отправитель планирует повторную передачу, если подтверждение (ACK) не получено.

Функция DCF широко поддерживается и используется, в то время как PCF является полной противоположностью. Функции DCF и PCF могут сосуществовать в одной и той же радиочастотной среде, например, ваша сеть и сеть соседней компании могут работать в рамках DCF и PCF независимо. Однако конструктивно такое сосуществование достигается за счет передачи приоритета передачи от устройств DCF устройствам PCF. В частности, центральный координатор сети WLAN с PCF после освобождения среды может получить доступ к ней раньше, чем устройства DCF. Следовательно, сети WLAN PCF статистически обладают более высокой производительностью и более высокой пропускной способностью, чем сети WLAN DCF в среде со смешанным режимом. В загруженной среде WLAN разница может быть более заметной.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает использование протоколов DCF и PCF. Когда используются оба протокола доступа к среде, приложение AirMagnet WiFi Analyzer повышает осведомленность о нарушении режима работы протокола DCF.

Reserved MGMT/CTRL Frames (Зарезервированные кадры MGMT/CTRL)

Описание сигнала тревоги и возможные причины

Беспроводной трафик содержит передачу небольших единиц информации, известных как «кадры», которые передаются между устройствами, поддерживающими беспроводную связь. Спецификация 802.11 классифицирует большинство беспроводных кадров по трем основным типам, определяемым двухбитовым полем, содержащимся в составе каждого кадра. Основными типами кадров являются:

- DATA - Кадры данных (определяемые битовым кодом 10) используются для большинства фактических передач данных в сети.
- CTRL - Кадры управления (определяемые битовым кодом 01) используются для управления доступом устройств к беспроводной среде. Примерами кадров CTRL являются кадры готовности к передаче (RTS), готовности к приему (CTS) и подтверждения (ACK).
- MGMT - Кадры менеджмента (определяемые битовым кодом 00), которые несут информацию, относящуюся к транзакциям между беспроводными устройствами (например, об аутентификации, поддерживаемых скоростях и т.д.). Эти кадры включают в себя, среди прочего, запросы подключения, сигналы маяка и ответы на зондирование.

После того, как тип кадра установлен, он далее классифицируется по подтипу, определяемому четырьмя битами, следующими за битовым кодом его типа (например, кадр Probe Request (Зондирующий запрос) использует битовый код подтипа 0100). В спецификации 802.11 используются не все возможные четырехбитовые варианты, но те, что не используются активно, считаются «зарезервированными» и, как таковые, никогда не должны отображаться в беспроводном трафике. Обнаружение кадров с использованием зарезервированного подтипа может указывать на неправильно настроенное устройство или попытку злоумышленника остаться незамеченным в беспроводной сети.

В связи с прямым влиянием на сетевую активность важно, чтобы кадры MGMT и CTRL использовали соответствующие подтипы, заданные в спецификации 802.11. Использование кадрами зарезервированных подтипов может вызвать снижение пропускной способности из-за избыточного количества кадров в эфире, а в худшем случае потенциально могут вызвать сбои в работе некоторых сетевых устройств.

Решение AirMagnet

Устройства, передающие кадры MGMT или CTRL с использованием зарезервированных подтипов, могут указывать на дефект или ошибку в настройке конфигурации устройства. Наличие таких устройств может привести к тому, что корпоративная сеть будет считаться не соответствующей определенным региональным нормам. Следовательно, важно изменить конфигурацию устройства в соответствии со спецификациями стандарта 802.11.

EAP TLS Bad Packet (Плохой пакет EAP TLS)

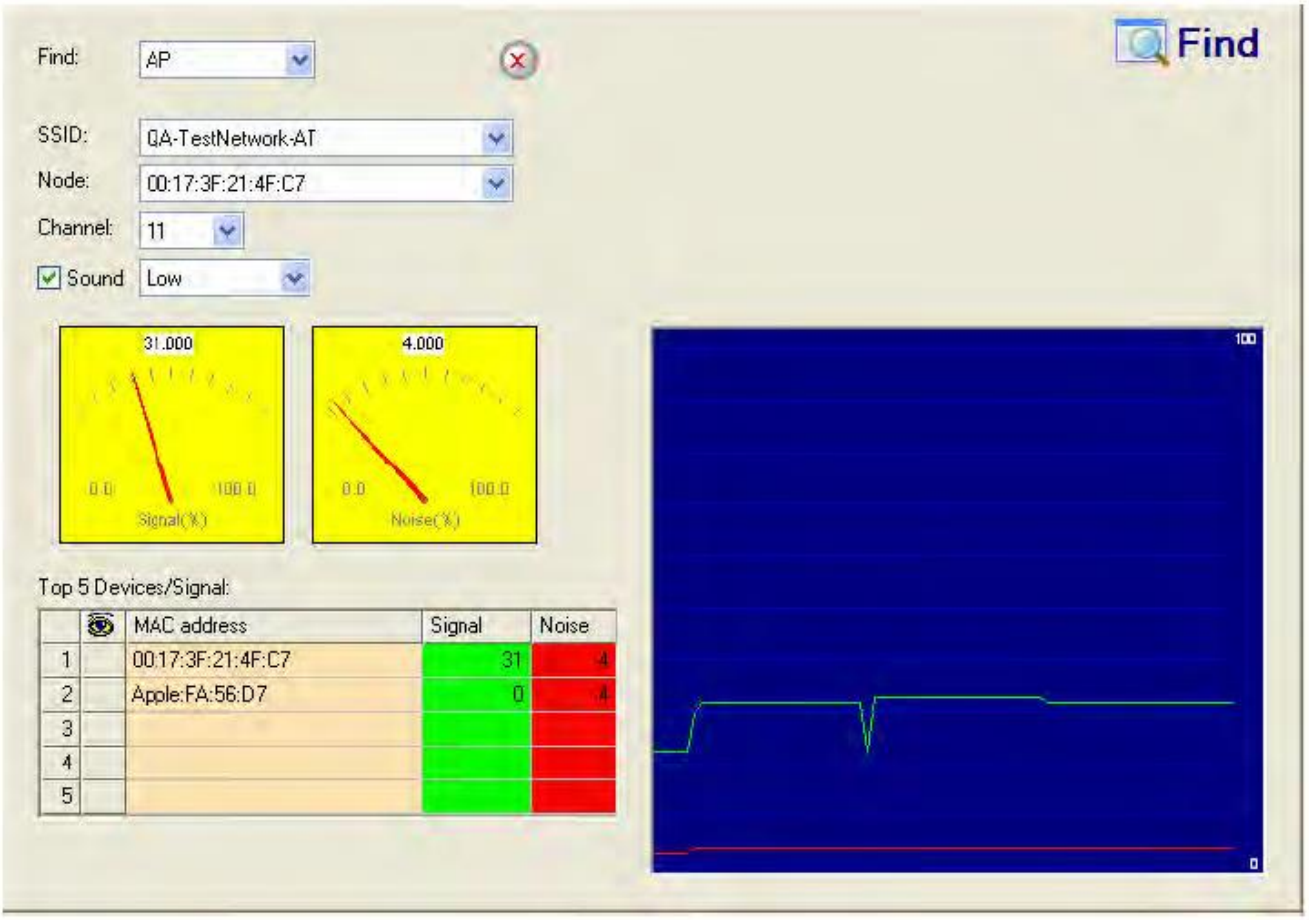
Описание сигнала тревоги и возможные причины

Протокол расширенной аутентификации (Extensible Authentication Protocol - EAP) - это базовая структура безопасности, которая улучшает шифрование транзакций 802.11. Данная структура может сочетаться с широким спектром различных механизмов аутентификации, включая известную версию Transport Layer Security (TLS) (Безопасность транспортного уровня), протокол на основе сертификатов. По сравнению со стандартными сеансами аутентификации с совместно используемым ключом и паролем механизм EAP-TLS обеспечивает дополнительную безопасность, создавая новый ключ для каждого сеанса. Это означает, что каждое активное соединение с точкой доступа, использующей аутентификацию EAP-TLS, создает новый совместно используемый ключ исключительно для этого соединения, что делает протокол значительно более надежным для защиты от злоумышленников по сравнению со стандартными механизмами совместно используемого ключа.

Каждый кадр EAP содержит заголовок пакета, состоящий из трех основных флажков: кода, идентификатора и длины. Для проведения попыток проникновения в беспроводные сети злоумышленники могут подделывать пакеты EAP, в которых используются эти флажки, включая те попытки, что могут привести к сбою определенных моделей точек доступа при использовании аутентификации EAP-TLS. Злоумышленник может воспользоваться подобной уязвимостью, передав дефектные кадры на корпоративную точку доступа. Посредством отправки пакетов EAP-TLS с флажком идентификатора, установленным на «c0», и без заданной длины сообщения TLS или данных, можно вывести из строя точки доступа некоторых производителей до момента их последующей перезагрузки. Во время перезагрузки у злоумышленников может появиться возможность получить доступ к корпоративной сети, что приведет к потере безопасности.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает передачи EAP-TLS и запускает сигнал тревоги при обнаружении дефектных или недействительных кадров. Хотя эта проблема не всегда может свидетельствовать об атаке на беспроводную сеть, для поддержания работоспособности сети ее все равно следует устранить. Чтобы отследить источник ошибочных кадров и определить основную причину проблемы, системным администраторам рекомендуется использовать инструмент Find (Найти).



HT-Intolerant Degradation of Service (Ухудшение обслуживания из-за нетерпимости HT)

Описание сигнала тревоги и возможные причины

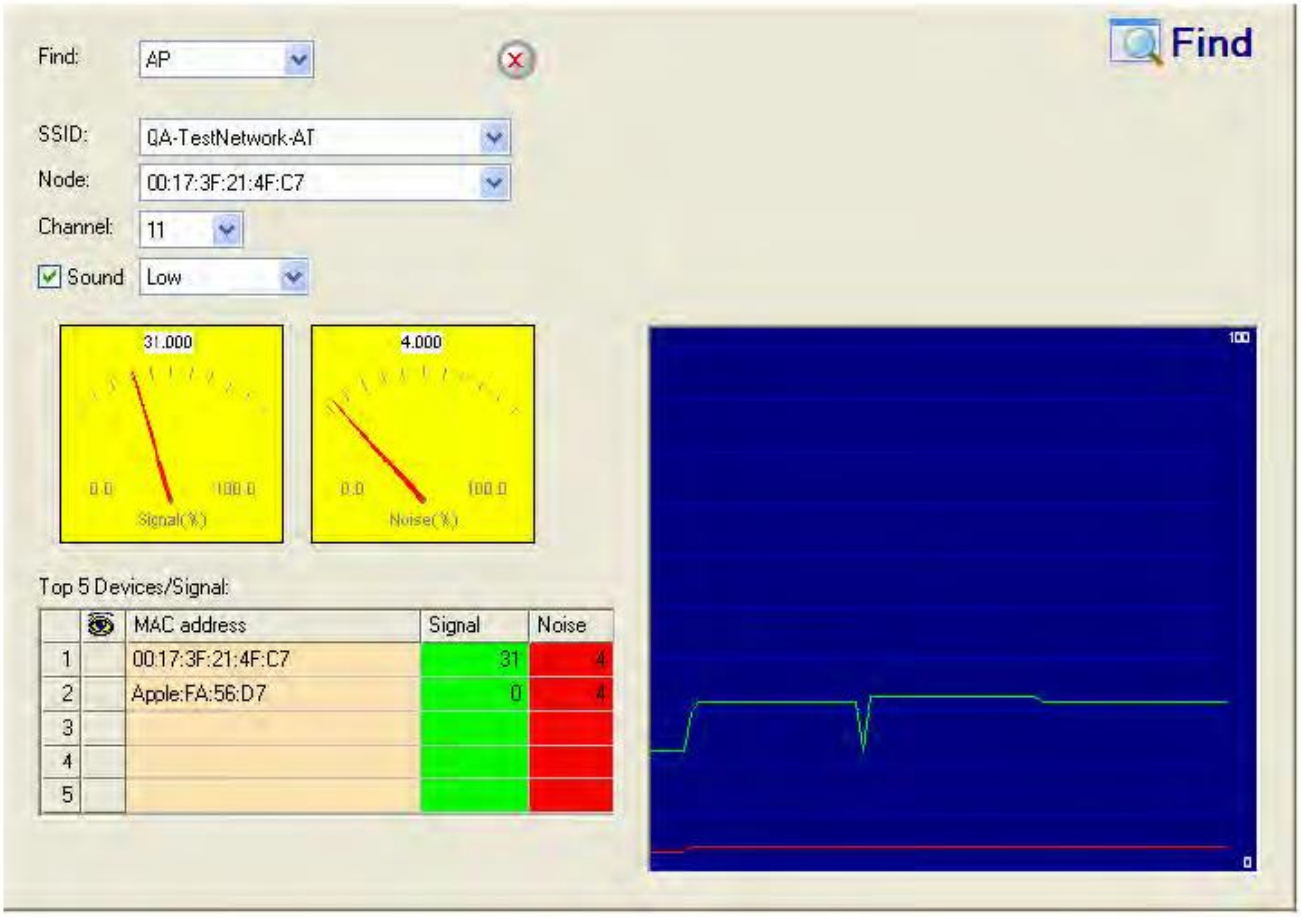
Внедрение стандарта беспроводной связи 802.11n предоставляет использующим беспроводную сеть предприятиям потенциальную возможность увеличения дальности и скорости беспроводной связи по сравнению с предыдущими реализациями стандарта (802.11a/b/g). Частично это связано с тем, что устройства 802.11n способны осуществлять передачу по гораздо более широкому каналу (40 МГц) по сравнению с каналом 20 МГц, который использовался в предшествующих стандартах.

Однако для обеспечения необходимой обратной совместимости с устаревшими устройствами, присутствующими в большинстве беспроводных сетей, в стандарте 802.11n используется специальная функция, позволяющих указать для устройств, используют ли они каналы 20 или 40 МГц. В стандартном кадре запроса подключения (который передается каждый раз, когда устройство пытается установить связь с точкой доступа), устройство может передавать флажок «HT intolerant» (Нетерпимо к HT), который заставит точку доступа вернуться в стандартный режим 20 МГц. Хотя это позволяет устройству беспроводно взаимодействовать с точкой доступа, данный переключатель заставляет точку доступа оставаться в режиме 20 МГц в течение как минимум 30 минут (30-минутный таймер сбрасывается каждый раз, когда принимается флажок «HT intolerant»). В течение этого времени устройства, которые могут работать на каналах 40 МГц стандарта 802.11n, будут при подключении к точке доступа принудительно переводиться в режим 20 МГц. Это сводит на нет повышенную скорость, которая является одним из основных преимуществ развертывания сетей 802.11n.

Атакующие беспроводную сеть злоумышленники могут воспользоваться флажком «HT intolerant», отправив кадр запроса подключения на точку доступа 802.11n, тем самым вынуждая её уменьшить ширину своего канала (и, следовательно, максимальную скорость передачи). Обратите внимание, что злоумышленнику не обязательно успешно подключаться к точке доступа. Для ухудшения обслуживания всех устройств, связанных с атакуемой точкой доступа, достаточно отправки самого запроса на подключение.

Решение AirMagnet

Важно убедиться, что устаревшие устройства либо исключены из сети стандарта 802.11n, либо в рамках развертывания сети подключены к другим устаревшим точкам доступа. Хотя этот сигнал тревоги не обязательно указывает на атаку беспроводной сети (поскольку может возникать просто из-за наличия устаревшего устройства в среде), снижение скорости может ухудшить общую производительность сети. В случае если проблему вызывает легитимное устройство, рекомендуется обнаружить его и настроить для него соединение с другими устаревшими устройствами. Отследить источник кадров устаревшего стандарта для быстрого разрешения проблемы поможет инструмент Find (Найти).



Denial-of-Service Attack: Block ACK (Атака типа «отказ в обслуживании»: подтверждение блока)

Описание сигнала тревоги и возможные причины

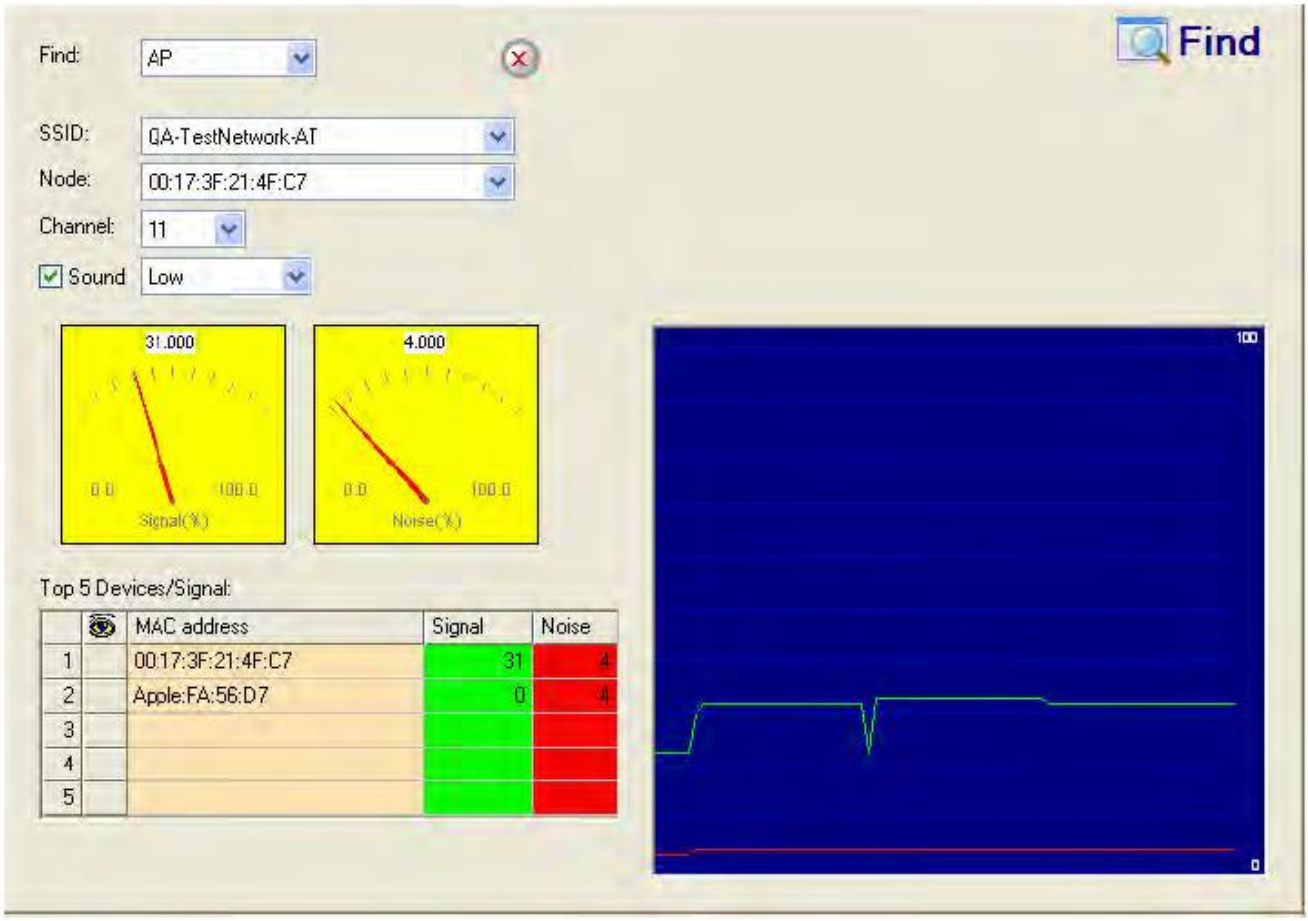
В устаревших сетях (до стандарта 802.11n) от устройств требуется отправлять кадр подтверждения ACK для каждого полученного кадра, в результате чего большой процент трафика в сети приходится на служебные данные. Такое неэффективное использование пропускной способности сети было учтено в спецификации 802.11n, в которой был введен новый тип кадра, называемый кадром Block ACK (Подтверждение блока). Механизм Block ACK позволяет точке доступа с помощью одного кадра ACK подтверждать блоки из нескольких кадров, тем самым уменьшая объем сетевых служебных данных.

Форма DoS-атаки, использующая преимущества этого процесса, позволяет злоумышленнику предотвратить получение точкой доступа стандарта 802.11n кадров от легитимного корпоративного клиента. Чтобы инициировать обмен Block ACK, клиент отправляет на точку доступа кадр ADDBA (добавить подтверждение блока). Кадр ADDBA содержит порядковые номера, сообщающие точке доступа размер передаваемого блока. После этого точка доступа примет все кадры, которые попадают в заданную последовательность (следовательно, отбросит любые кадры, выходящие за пределы диапазона), и по завершению транзакции передаст сообщение BlockACK обратно клиенту.

Для использования этого процесса злоумышленник может передать недопустимый кадр ADDBA, подделав MAC-адрес легитимного клиента. После получения этого сообщения точка доступа останется закрытой для всего трафика за пределами диапазона, указанного (подделанным) кадром ADDBA. Тем самым обмен данными с легитимным клиентом на точке доступа будет закрыт. Этот процесс заставит точку доступа постоянно игнорировать любой передаваемый от клиента трафик до тех пор, пока не будет удовлетворен недопустимый диапазон кадров. Это позволит злоумышленнику заблокировать клиента на неопределенный период времени.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает транзакции ADDBA на наличие признаков подделки клиентской информации. Когда обнаруживается, что злоумышленник пытается инициировать атаку с использованием Block ACK, срабатывает сигнал тревоги, идентифицирующий MAC-адреса устройства злоумышленника и устройства жертвы. Чтобы найти атакующее устройство и отключить атаку или иным образом удалить его из беспроводной среды, используйте инструмент Find (Найти).



Хотя при необходимости устройства, использующие для инициирования атак функцию ADDBA, можно устранить в каждом конкретном случае, единственным надежным способом полностью устранить угрозу является отключения механизма ADDBA на точках доступа, используемых в беспроводной среде. За необходимыми инструкциями по настройке обратитесь к документации производителя точки доступа.

AP PHY Data Rate Changed (Изменена скорость передачи данных физического уровня на точке доступа)

Описание сигнала тревоги и возможные причины

Под скоростью передачи данных точки доступа понимается скорость, с которой устройство передает данные в беспроводной среде. В большинстве сетей используемая скорость передачи данных - это максимальное значение, доступное для типа среды, используемой большинством устройств в сети (то есть устройства 802.11a/g обычно имеют максимальную скорость 54 Мбит/с; устройства 802.11n имеют максимальную скорость 600 Мбит/с). Это значение объявляется в кадрах маяка и ответах на зондирование, передаваемых каждой точкой доступа.

Некоторые производители точек доступа корпоративного уровня позволяют пользователям вручную указывать скорости передачи данных, на которых точка доступа может осуществлять передачу. Подобная настройка конфигурации может быть полезна для того, чтобы предотвратить падение используемых скоростей ниже указанного порогового значения. Ограничивая доступную для точки доступа скорость, пользователи также могут препятствовать подключению «устаревших» устройств (например, использующих технологию 802.11b) к более новым корпоративным точкам доступа. Поскольку подключения устаревших устройств могут заставить точки доступа передавать данные с более низкой скоростью для всех устройств, одно соединение 802.11b способно отрицательно повлиять на все устройства, связанные с той же точкой доступа.

В сетях, использующих настройку скорости передачи данных, неавторизованные изменения поддерживаемых скоростей могут привести к снижению пропускной способности и надежности беспроводной сети.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает список скоростей, поддерживаемых корпоративными точками доступа, сравнивая сигналы маяков и ответы на зондирование, чтобы убедиться в отсутствии каких-либо изменений. При обнаружении изменений срабатывает сигнал тревоги «AP Data Rate Changed», уведомляющий ИТ-персонал о проблеме.

Неавторизованные или неожиданные изменения конфигурации корпоративных точек доступа могут указывать на потенциальное нарушение безопасности. Пользователям рекомендуется как можно скорее определить причину изменений и восстановить конфигурацию точки доступа в соответствии с корпоративными стандартами.

AP PHY Data Rate Anomaly (Аномалия скорости передачи данных физического уровня на точке доступа)

Описание сигнала тревоги и возможные причины

Под скоростью передачи данных точки доступа понимается скорость, с которой устройство передает данные в беспроводной среде. В большинстве сетей используемая скорость передачи данных - это максимальное значение, доступное для типа среды, используемой большинством устройств в сети (то есть устройства 802.11a/g обычно имеют максимальную скорость 54 Мбит/с). Это значение объявляется в кадрах маяка и ответах на зондирование, передаваемых каждой точкой доступа.

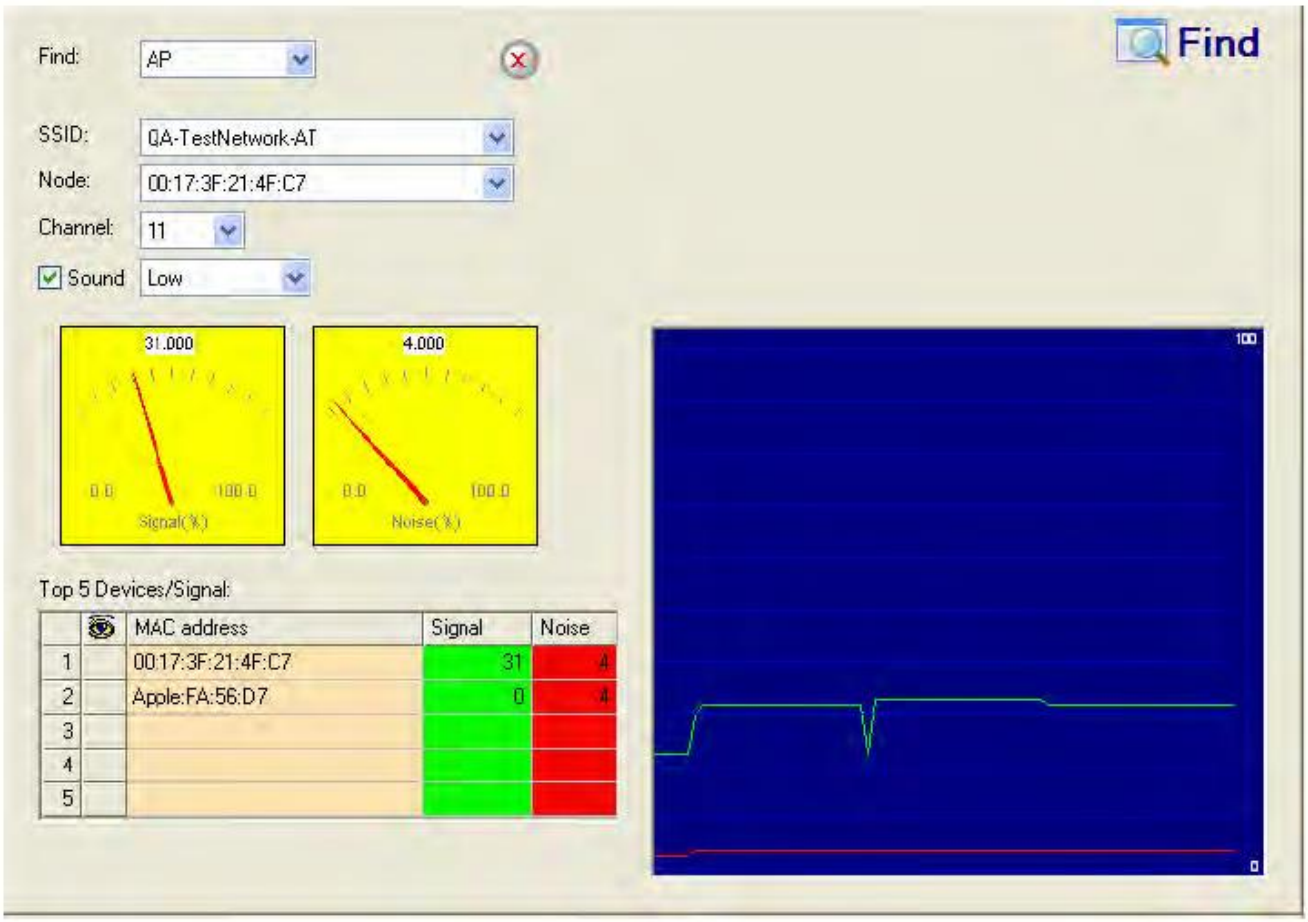
Некоторые производители точек доступа корпоративного уровня позволяют пользователям вручную указывать скорости передачи данных, на которых точка доступа может осуществлять передачу. Подобная настройка конфигурации может быть полезна для того, чтобы предотвратить падение используемых скоростей ниже указанного порогового значения. Ограничивая доступную для точки доступа скорость, пользователи также могут препятствовать подключению «устаревших» устройств (например, использующих технологию 802.11b) к более новым корпоративным точкам доступа. Поскольку подключения устаревших устройств могут заставить точки доступа передавать данные с более низкой скоростью для всех устройств, одно соединение 802.11b способно отрицательно повлиять на все устройства, связанные с той же точкой доступа.

В сетях, использующих настройку скорости передачи данных, неавторизованные изменения поддерживаемых скоростей могут привести к снижению пропускной способности и надежности беспроводной сети.

Кроме того, в сетях, где требуется соблюдение нормативных требований (таких как HIPAA, Sarbanes-Oxley и т.д.), одна не соответствующая указанным правилам точка доступа может привести к нарушению корпоративной политики во всей сети.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer позволяет пользователю указать поддерживаемые скорости передачи данных для всех известных точек доступа. Если устройство обнаруживает передачу с неавторизованной скоростью, срабатывает сигнал тревоги «AP Data Rate Anomaly». Для нахождения источника проблемы и исключения его из беспроводной сети системным администраторам рекомендуется использовать инструмент Find (Найти).



Кроме того, пользователи должны определить, связаны ли какие-либо распознанные корпоративные беспроводные клиенты с неавторизованной точкой доступа, поскольку эти станции могли передавать конфиденциальные данные через незащищенное устройство.

Device Unprotected by EAP-TLS (Устройство не защищено протоколом EAP-TLS)

Описание сигнала тревоги и возможные причины

Протокол расширенной аутентификации (Extensible Authentication Protocol - EAP) - это базовая структура безопасности, которая улучшает шифрование транзакций 802.11. Данная структура может сочетаться с широким спектром различных механизмов аутентификации, включая известную версию Transport Layer Security (TLS) (Безопасность транспортного уровня), протокол на основе сертификатов. По сравнению со стандартными сеансами аутентификации с совместно используемым ключом и паролем механизм EAP-TLS обеспечивает дополнительную безопасность, создавая новый ключ для каждого сеанса. Это

означает, что каждое активное соединение с точкой доступа, использующей аутентификацию EAP-TLS, создает новый совместно используемый ключ исключительно для этого соединения, что делает протокол значительно более надежным для защиты от злоумышленников по сравнению со стандартными механизмами совместно используемого ключа.

Устройства, настроенные на использование протокола EAP, но не имеющие механизма аутентификации TLS, могут являться потенциально небезопасными подключениями к беспроводной сети. Можно использовать ряд альтернативных существующих механизмов (например, EAP-TTLS или EAP-FAST), которые обычно обеспечивают большее удобство, чем EAP-TLS, но за счет снижения безопасности сети. Хотя такие механизмы дают конечным пользователям возможность легкого и быстрого подключения, в результате также злоумышленники могут получить доступ к критически важным корпоративным данным. Злоумышленникам проще перехватить и декодировать обмен EAP, который не защищен аутентификацией TLS, что может привести к утечке конфиденциальных данных, отправленных легитимным пользователем.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает транзакции EAP для обнаружения любых устройств, которые не реализуют механизм TLS, и запускает сигнал тревоги, чтобы уведомить администраторов об уязвимости. Отображаемый на экране AirWISE текст сигнала тревоги идентифицирует проблемное устройство, а также используемый альтернативный механизм аутентификации. ИТ-персоналу рекомендуется найти вызывающее тревогу устройство и настроить на нем использование механизма EAP-TLS.

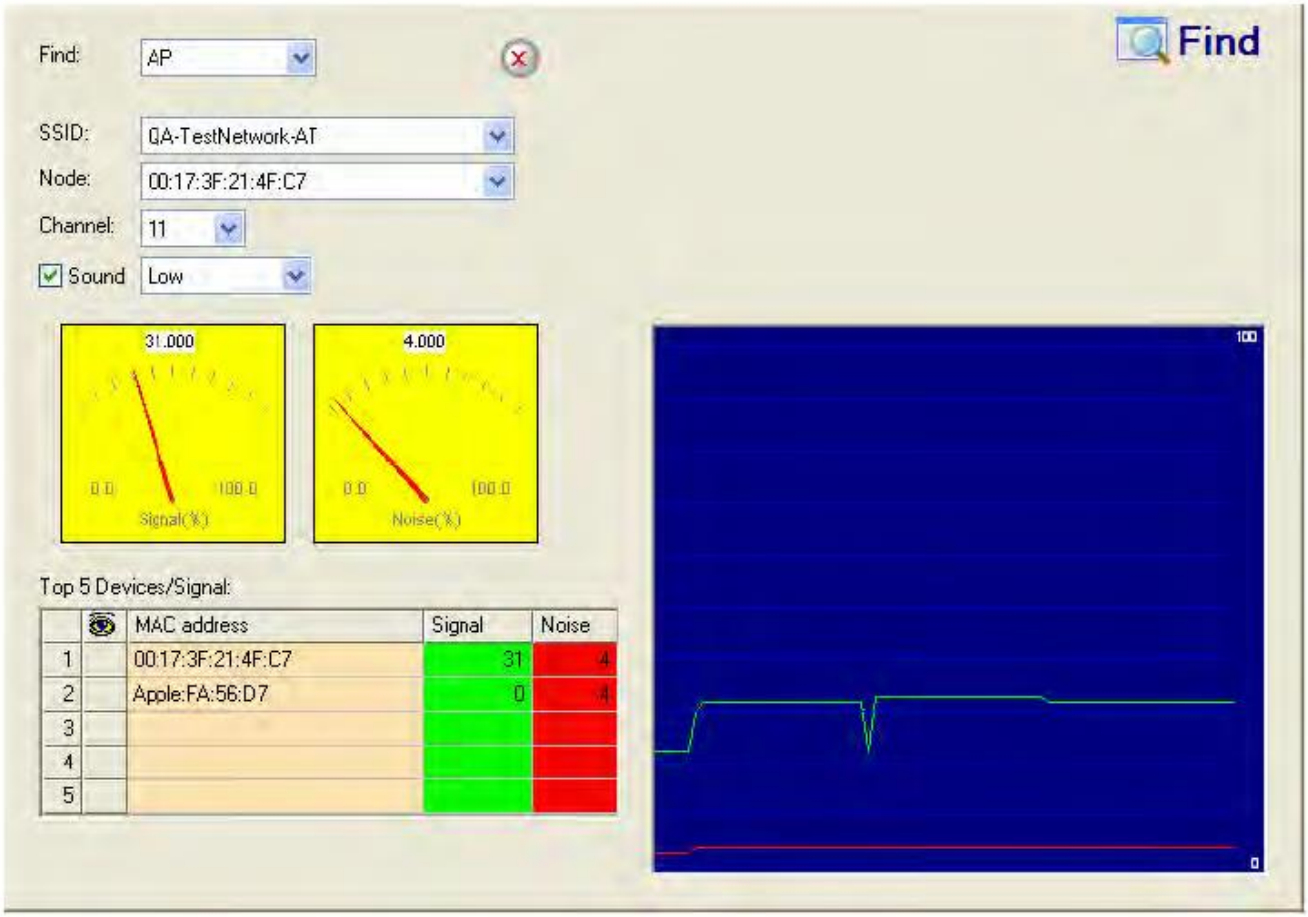
Denial-of-Service Attack: Probe Request Flood (Атака типа «отказ в обслуживании»: флуд с использованием зондирующих запросов)

Описание сигнала тревоги и возможные причины

При попытке установить связь с беспроводной точкой доступа станция должна сначала передать кадр зондирующего запроса, который позволит определить возможности любых беспроводных устройств в окружающей среде. В стандартной сети принявшая подобный запрос точка доступа передаст кадр ответа на зондирование, содержащий различные данные (такие как скорости передачи данных, поддерживаемые точкой доступа, требования аутентификации и т.д.), после чего станция может перейти к запросу подключения.
Данная процедура представляет собой потенциальную уязвимость в транзакциях 802.11, которую можно использовать в атаке на беспроводную сеть. В любой сети, если точка доступа получает кадр зондирующего запроса, она автоматически отвечает кадром ответа на зондирование. Следовательно, если на точку доступа передается слишком много подобных запросов, она может быть заблокирована от обслуживания других клиентов из-за необходимости передачи огромного объема ответов на зондирование.
DoS-атака (атаки типа «отказ в обслуживании») позволяет злоумышленнику заставить целевую точку доступа формировать постоянный поток ответов на зондирование, предназначенных для обслуживания несуществующих клиентов. Во время лавинной рассылки (флуда) зондирующих запросов злоумышленник генерирует большое количество запросов, отправляемых с некоторого набора «поддельных» MAC-адресов, нацеленных на конкретную точку доступа. В результате постоянно отвечающая на ложные запросы точка доступа зависнет, что приведет к отказу в обслуживании для всех клиентов, беспроводное обслуживание которых зависит от этой точки доступа.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает уровень обнаруженных кадров зондирующих запросов и при превышении порогового значения запускает сигнал тревоги о лавинной рассылке (флуде) зондирующих запросов. Представленное на экране AirWISE описание тревоги будет включать либо MAC-адрес станции, передающей зондирующие запросы, либо адрес атакуемой точки доступа. Для наблюдения за количеством обнаруженных кадров пробных запросов и определения их источника системным администраторам рекомендуется использовать экран Infrastructure (Инфраструктура). Даже в случаях, когда запросы поступают от легитимных станций, увеличение объема трафика управления в сети может привести к снижению пропускной способности и скорости для авторизованных пользователей. Для нахождения устройства, с которого выполняется атака, и удаления его из сети ИТ-персоналу нужно воспользоваться инструментом Find (Найти).



Имейте в виду, что злоумышленники часто подделывают MAC-адрес легитимной станции, уже присутствующей в сети. В таком случае подобную станцию следует отключить, чтобы ее сигнал не мешал обнаружению злоумышленника.

Denial-of-Service Attack: Probe Response Flood (Атака типа «отказ в обслуживании»: флуд с использованием ответов на зондирование)

Описание сигнала тревоги и возможные причины

При попытке установить связь с беспроводной точкой доступа станция должна сначала передать кадр зондирующего запроса, который позволит определить возможности любых беспроводных устройств в окружающей среде. В стандартной сети принявшая подобный запрос точка доступа передаст кадр ответа на зондирование, содержащий различные данные (такие как скорости передачи данных, поддерживаемые точкой доступа, требования аутентификации и т.д.), после чего станция может перейти к запросу подключения.
Данная процедура представляет собой потенциальную уязвимость в транзакциях 802.11, которую можно использовать в атаке на беспроводную сеть. Форма DoS-атаки (атаки типа «отказ в обслуживании») позволяет злоумышленнику предотвратить получение целевой станцией любых достоверных кадров ответа на зондирование от точек доступа в сети предприятия. Во время лавинной рассылки (флуда) ответов на зондирование злоумышленник генерирует большое количество ответов, отправляемых с серии «поддельных» MAC-адресов, нацеленных на определенную станцию. В результате станция, обрабатывающая поток поддельных кадров, не сможет идентифицировать достоверные ответы на зондирование, отправленные с корпоративных точек доступа. Возникает задержка, которая инициирует отказ в обслуживании, и станция будет неспособна подключиться к корпоративной сети.

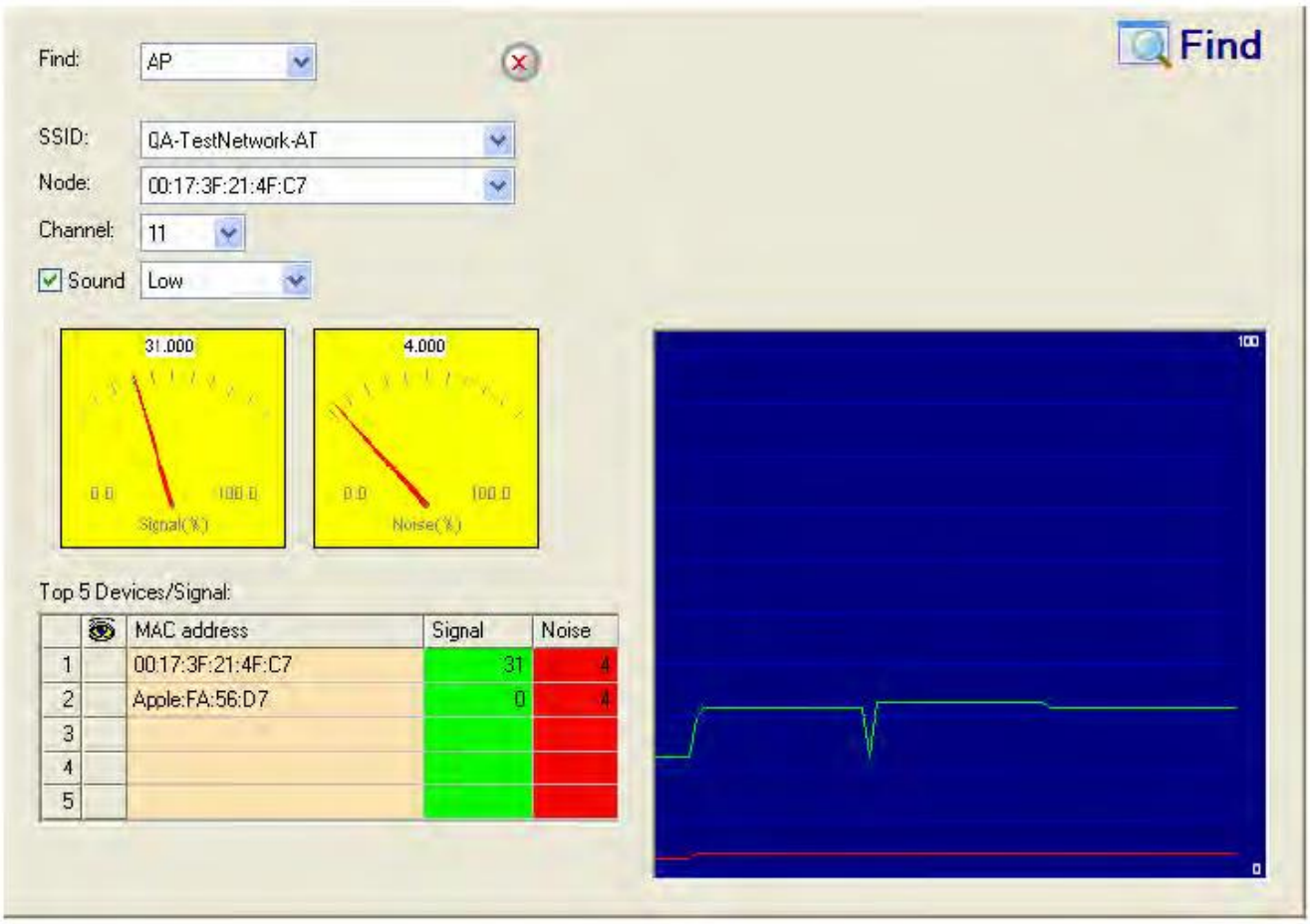
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает уровень кадров ответа на зондирование, передаваемых на станции в беспроводной среде, и запускает тревогу, если соблюдены два критерия:

- Количество кадров ответа на зондирование, переданных на данную станцию, превышает указанное пороговое значение, и

- Целевая станция не передавала кадр зондирующего запроса, означающий, что она ищет информацию о доступных точках доступа.

Даже в тех случаях, когда ответы достоверны, объем кадров таких ответов может вызвать проблемы с работой беспроводной сети, включая снижение пропускной способности и пропуск кадров из-за большого трафика управления. Поэтому атакующее устройство нужно обнаружить с помощью инструмента Find (Найти) и удалить из корпоративной среды.



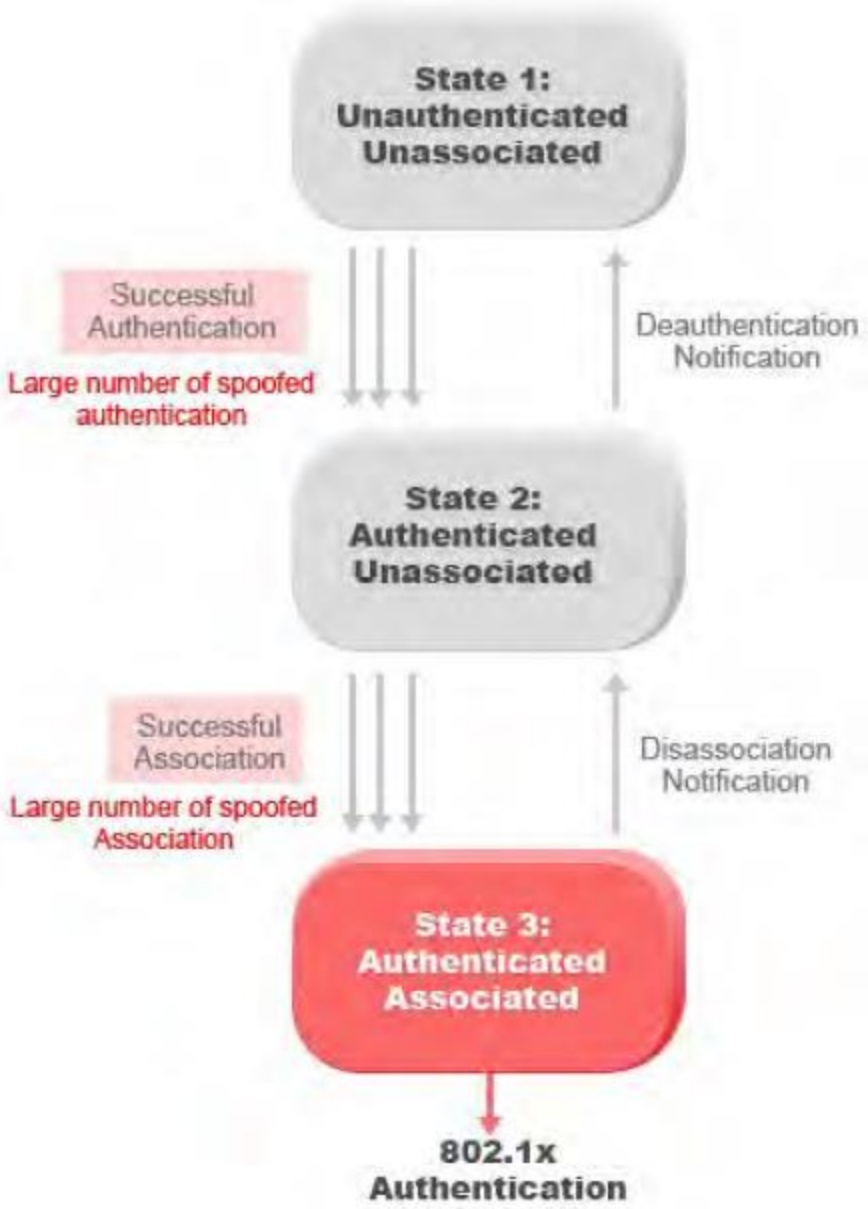
Denial-of-Service Attack: Re-Association Request Flood (Атака типа «отказ в обслуживании»: флуд с использованием запросов на повторное подключение)

Описание сигнала тревоги и возможные причины

Чтобы инициировать стандартное соединение 802.11, станция в беспроводной сети передает своей целевой точке доступа кадр запроса подключения. Соединение устанавливается после обмена соответствующими протоколами аутентификации, что позволяет станции получить доступ к сети. Если станция перемещается за пределы зоны покрытия сигнала начальной точки доступа, она попытается восстановить соединение с другой точкой доступа в той же сети. Для этого станция передает кадр запроса повторного подключения. Этот кадр сигнализирует второй точке доступа, что станция готова принять любые кадры, которые были помещены в буфер в течение периода переключения.

Во время аутентификации (до того, как станция будет готова для подключения), точка доступа сохраняет информацию о клиенте в своей таблице подключенных клиентов. Эта таблица представляет собой буферную память, предназначенную для того, чтобы точка доступа могла обрабатывать запросы на подключение (или повторное подключение) в порядке их получения. Хотя данный процесс эффективен в большинстве сетей, он представляет собой потенциальную уязвимость из-за того, что таблица подключения к точке доступа может быть заполнена ожидающими запросами на подключение клиентов. В этом случае точка доступа не сможет обслуживать новых пользователей, пока ожидающие запросы не будут удалены.

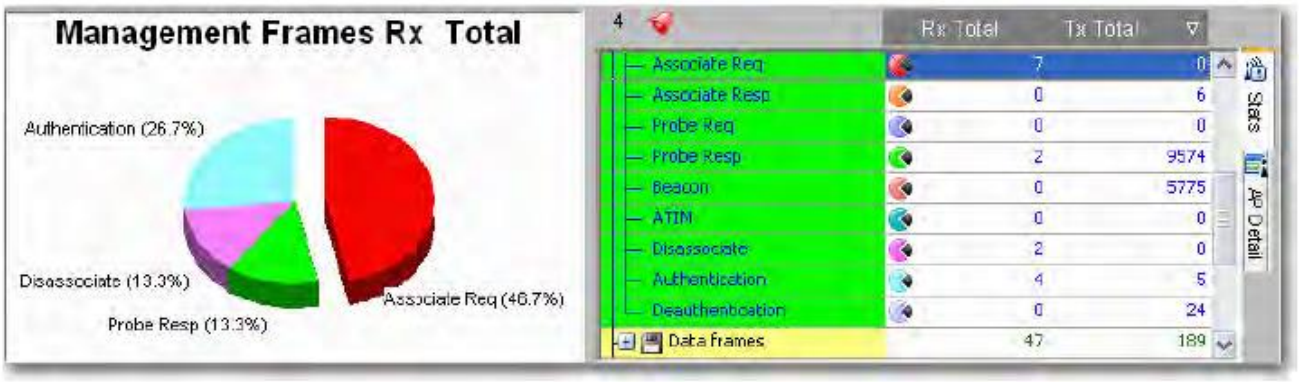
Одной из форм DoS-атаки (атаки типа «отказ в обслуживании») является исчерпание ресурсов точки доступа, в частности таблицы подключения клиентов, путем лавинной передачи (флуда) на точку доступа большого количества поддельных запросов на повторное подключение клиентов. Злоумышленник может заполнить таблицу подключения клиентов точки доступа, создав множество клиентов, достигающих состояния 3, как показано на рисунке ниже. После переполнения таблицы подключения клиентов легитимные клиенты не смогут подключиться к точке доступа, что и является целью атаки.



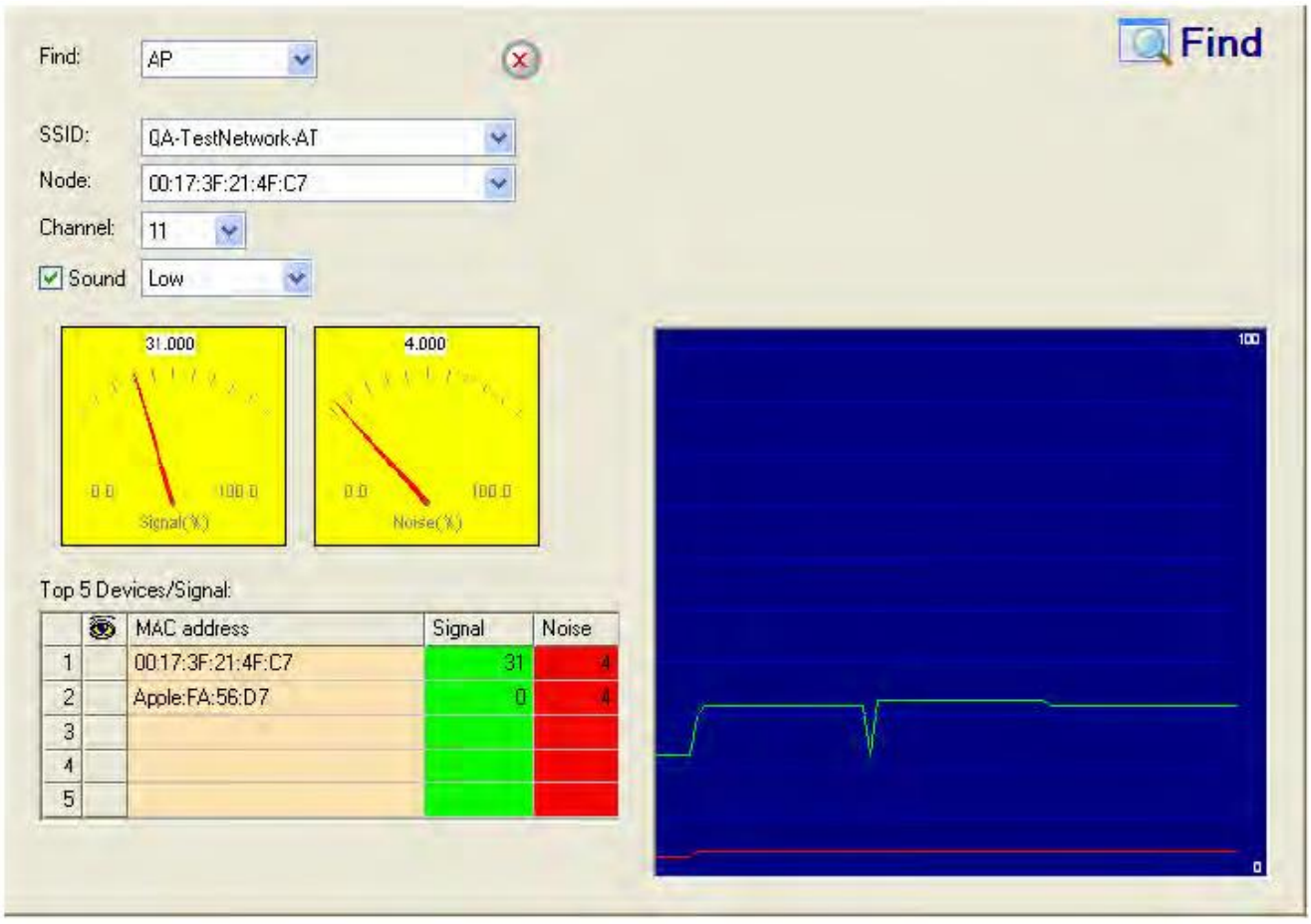
State 1: …	Состояние 1: Аутентификация не пройдена, нет соединения
Successful Authentication	Успешная аутентификация
Deauthentication Notification	Извещение о деаутентификации
Large number of spoofed authentication	Большое количество поддельных аутентификаций
State 2: …	Состояние 2: Аутентификация пройдена, нет соединения
Successful Association	Успешное подключение
Diassociation Notification	Извещение о разъединении
Large number of spoofed Association	Большое количество поддельных соединений
State 3:…	Состояние 3: Аутентификация пройдена, соединение установлено
802.1x Authentication	Аутентификация 802.1x

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает уровни кадров запроса повторного подключения в беспроводной среде и инициирует сигнал тревоги, если превышено пороговое значение для таких кадров. Эти кадры можно просмотреть на экране Infrastructure (Инфраструктура).



После определения источника избыточного количества кадров пользователям рекомендуется отследить устройство с помощью инструмента Find (Найти) и удалить его из сети предприятия.



Rogue AP by MAC Address (ACL) (Точка доступа, неавторизованная по MAC-адресу (ACL))

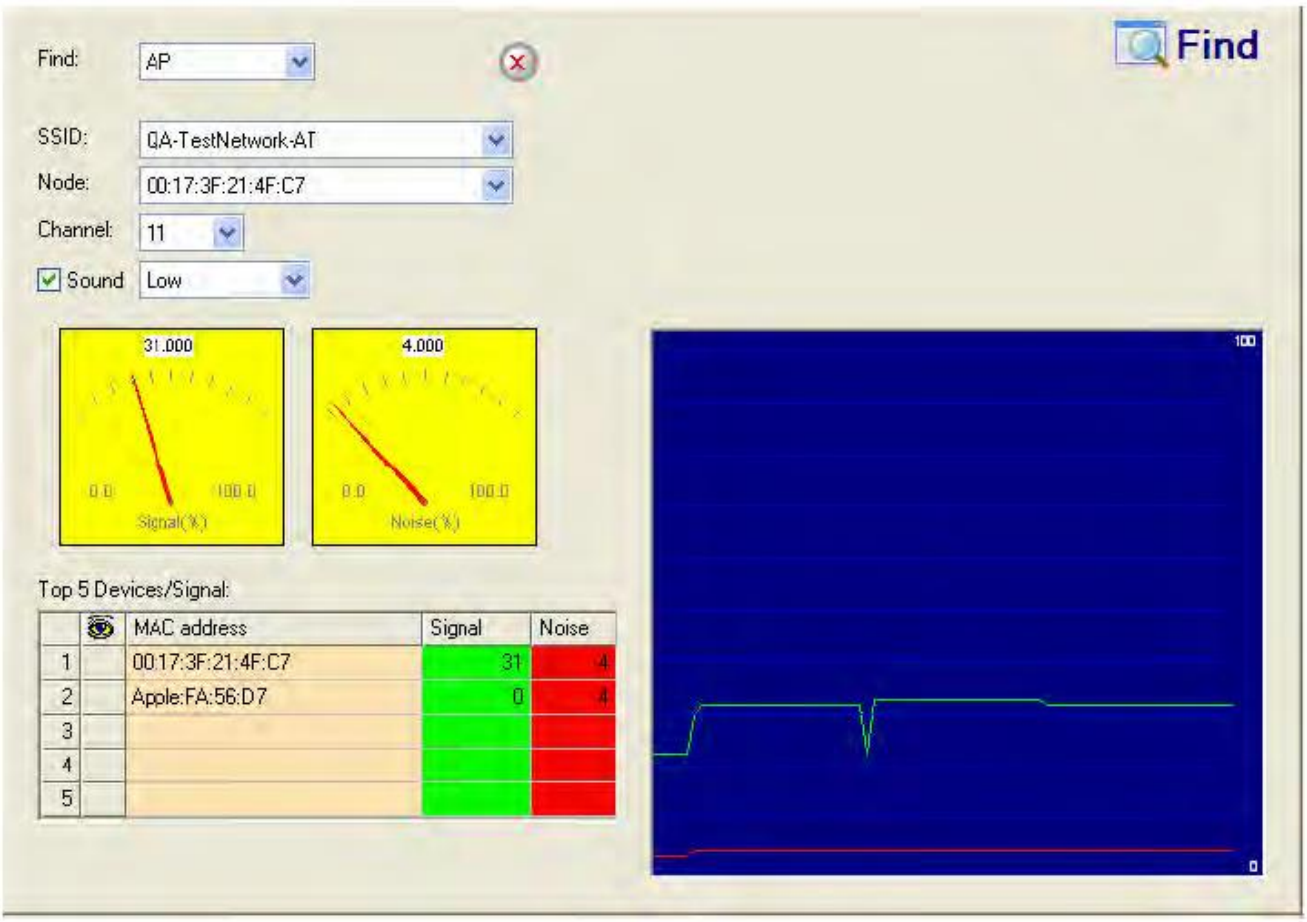
Описание сигнала тревоги и возможные причины

После настройки списка MAC-адресов авторизованных точек доступа приложение AirMagnet Wi-Fi Analyzer сможет предупреждать администраторов WLAN о неавторизованных (мошеннических) точках доступа, MAC-адрес которых не входит в предварительно настроенный список адресов. Список авторизованных MAC-адресов можно импортировать в приложение AirMagnet Enterprise из файла (AccessControl.txt). Этот файл является общим для точек доступа, станций сетевой инфраструктуры и устройств Ad-hoc. Его также можно генерировать автоматически, запросив приложение AirMagnet Enterprise принять все или определенное подмножество существующих точек доступа, обнаруженных датчиками AirMagnet SmartEdge.

Неавторизованные точки доступа, установленные неавторизованными сотрудниками, обычно не соответствуют стандартным корпоративным методам развертывания и могут поставить под угрозу безопасность как беспроводной, так и проводной сети. Сигнал тревоги Rogue AP может также указывать на попытки злоумышленников взломать проводную сеть предприятия. Следует тщательно изучать обнаруженные приложением AirMagnet Wi-Fi Analyzer неавторизованные устройства.

Решение AirMagnet

После обнаружения неавторизованной точки доступа и сообщения об этом от приложения AirMagnet WiFi Analyzer администратор WLAN может использовать инструмент FIND (Найти) для определения местонахождения неавторизованного устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Rogue AP Using Corporate SSID (Неавторизованная точка доступа, использующая корпоративный SSID)

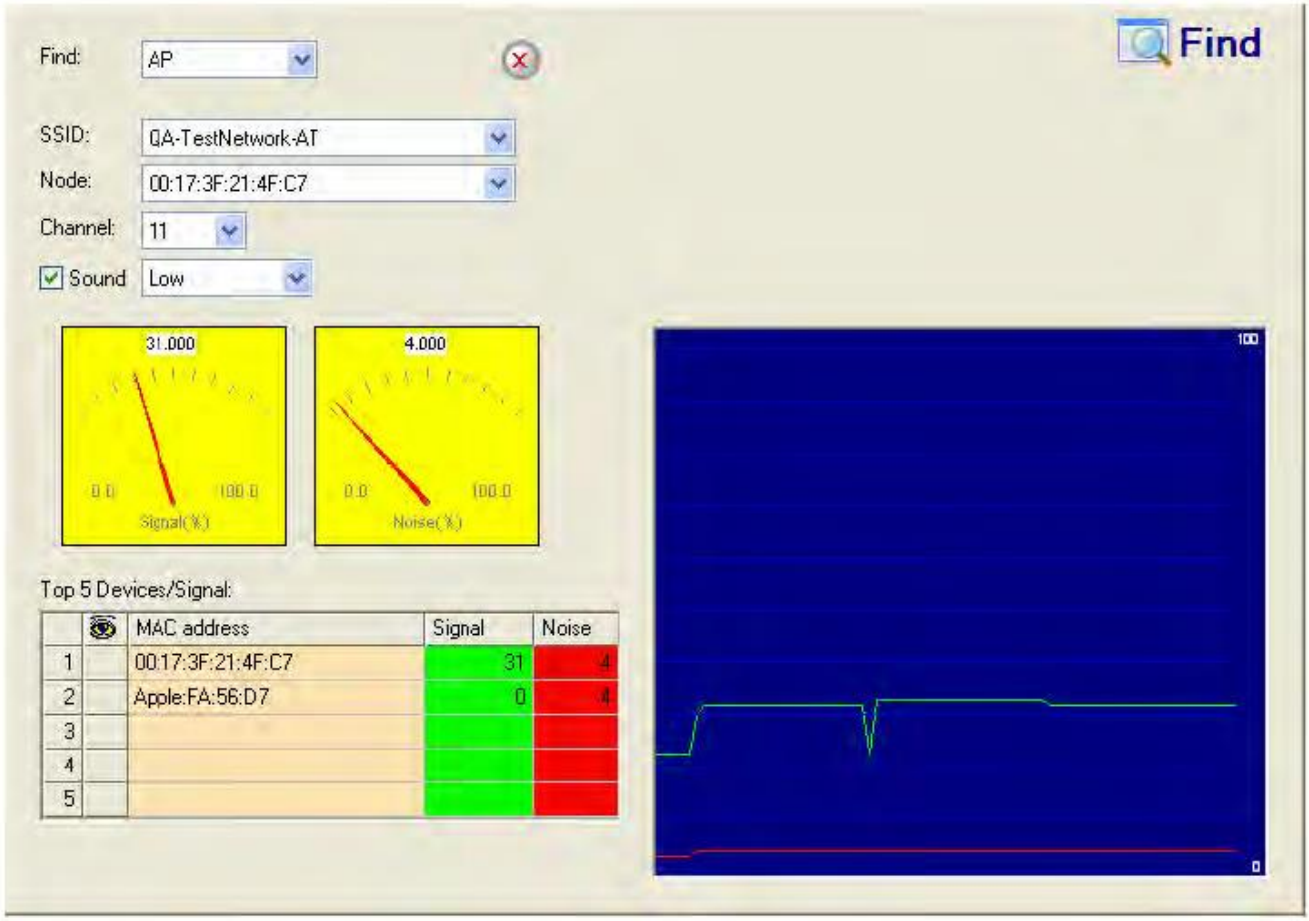
Описание сигнала тревоги и возможные причины

В большинстве корпоративных беспроводных сетей может использоваться несколько идентификаторов SSID для различных групп предполагаемых пользователей. Например, точки доступа могут устанавливаться с одним идентификатором SSID для корпоративных пользователей и другим отдельным идентификатором SSID для посетителей или сотрудников по контракту. Из-за разнообразия идентификаторов SSID, которое может существовать на корпоративных сетях, важно, чтобы пользователи могли контролировать среду и гарантировать, что любые неопознанные или неавторизованные идентификаторы SSID обнаруживаются и удаляются до того, как будет нарушена безопасность беспроводной сети.

Чтобы избежать обнаружения, злоумышленники могут настроить неавторизованную точку доступа с идентификатором SSID, который известен и легитимен в корпоративной среде. Если неавторизованная точка доступа не реализует механизмы аутентификации, требуемые корпоративной политикой, это может представлять угрозу безопасности сети. Опасность возникает, поскольку точка доступа использует действительный корпоративный идентификатор SSID, то есть может обманом заставить действующие станции подключаться к ней, что позволит злоумышленнику отслеживать любой трафик, передаваемый через незащищенные соединения.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает идентификаторы SSID, заданные в группе MyWLAN SSID, и запускает сигнал тревоги при обнаружении неизвестной или неавторизованной точки доступа, использующей корпоративный идентификатор SSID. Из-за потенциально высокого риска для безопасности пользователям рекомендуется найти неавторизованную точку доступа с помощью инструмента Find (Найти) и убедиться, что это легитимное устройство.



Rogue AP Operating in Greenfield Mode (Неавторизованная точка доступа, работающая в режиме Greenfield)

Описание сигнала тревоги и возможные причины

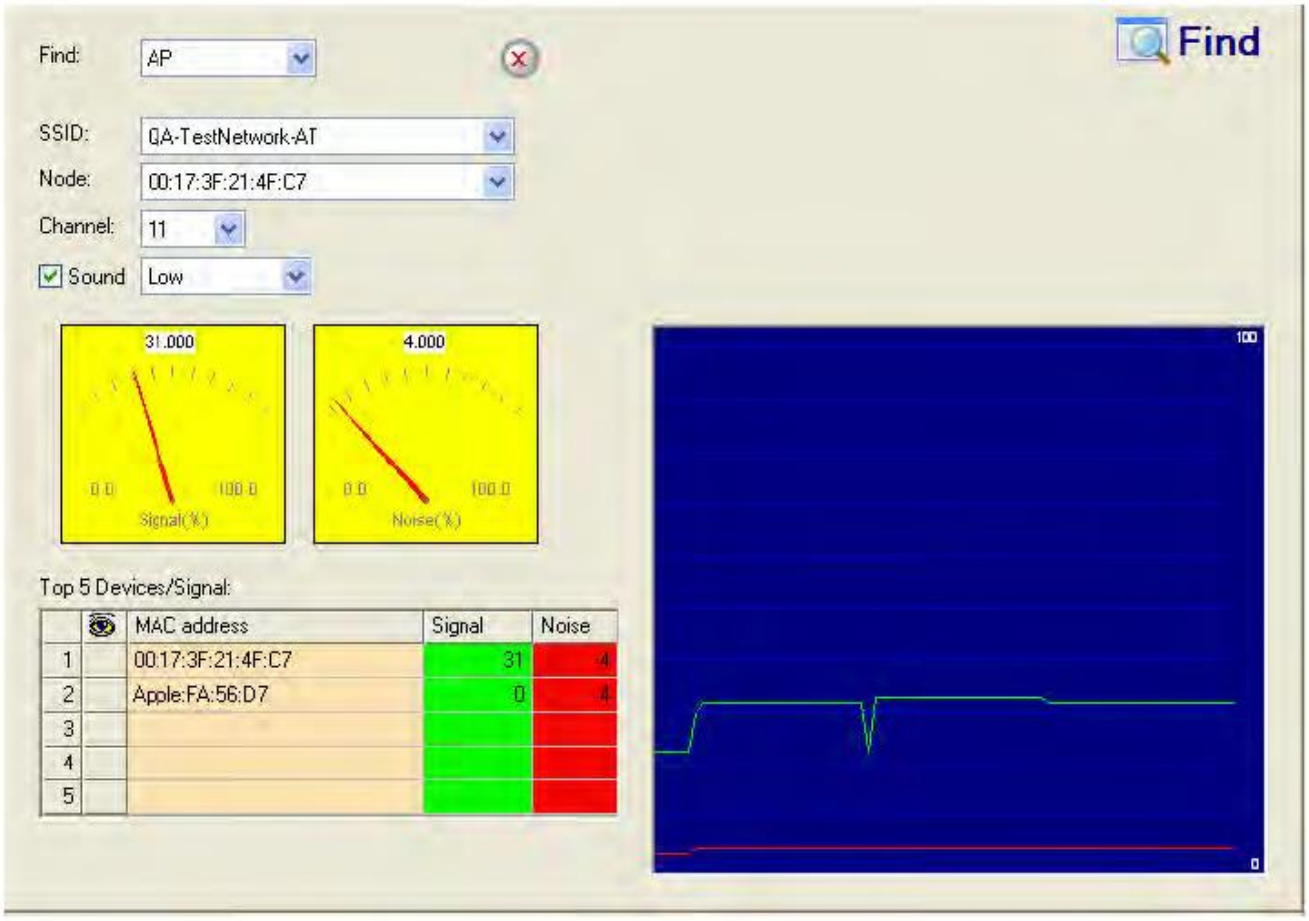
Спецификация 802.11n предоставляет пользователям возможность настраивать точки доступа 802.11n для использования режима Greenfield, который гарантирует, что к беспроводной сети смогут подключаться только устройства, поддерживающие скорости 802.11n. Этот механизм можно использовать для предотвращения потери скорости из-за используемых в беспроводной среде устаревших устройств (например, 802.11a/b/g). Устройства с включенным режимом Greenfield используют новую преамбулу кадра, которую не способны декодировать устаревшие устройства. За счет возможности подключения только устройств с поддержкой 802.11n точки доступа, работающие в режиме Greenfield, могут поддерживать скорость передачи до 300 Мбит/с. Если же допустить возможность подключения устаревших устройств, эта скорость упадет до максимального значения 54 Мбит/с.

Используемая устройствами Greenfield преамбула представляет потенциальную уязвимость в сетях, которые не используют совместимые с 802.11n системы обнаружения/предотвращения вторжений. Поскольку устаревшие устройства не могут декодировать новую преамбулу, защищенные системным мониторингом трафика 802.11a/b/g беспроводные сети не смогут обнаружить устройства, работающие в режиме Greenfield.

Чтобы воспользоваться этой уязвимостью, злоумышленник может настроить неавторизованную точку доступа для использования только в режиме Greenfield, и развернуть ее в сети, защищенной устаревшими устройствами обнаружения вторжений. Неавторизованная точка доступа будет невидима для существующей системы защиты, что позволит злоумышленнику спровоцировать подключение легитимных клиентов, поддерживающих стандарт 802.11n, к неавторизованной точке доступа. Это может предоставить злоумышленнику доступ к любой конфиденциальной информации, передаваемой от авторизованных клиентов.

Решение AirMagnet

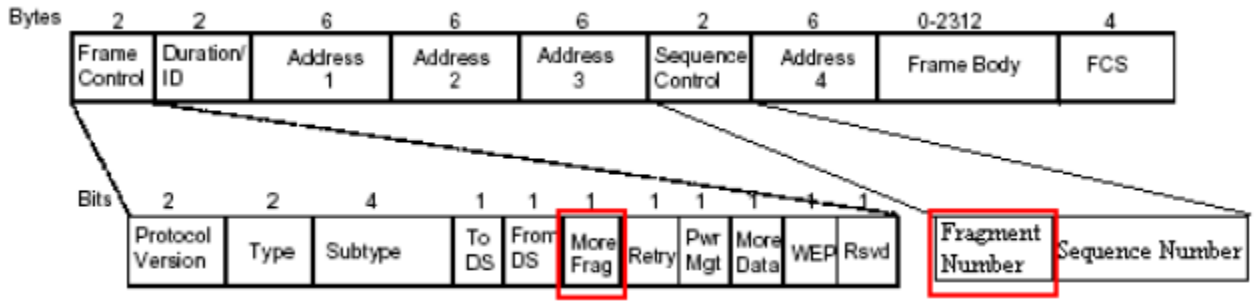
Защищенные устаревшими устройствами беспроводные сети не способны обнаружить устройства Greenfield. Для защиты от подобных атак пользователям следует обновить имеющуюся инфраструктуру обнаружения вторжений и развернуть устройства, способные отслеживать трафик 802.11n. При обнаружении неавторизованной точки доступа, работающей в режиме Greenfield, используйте инструмент Find (Найти), чтобы найти неавторизованное устройство и удалить его из сети.



Small Fragmented Frames Detected (Обнаружены мелкие фрагментированные кадры)

Описание сигнала тревоги и возможные причины

Уровень MAC стандарта 802.11 поддерживает процессы фрагментации и дефрагментации. Процесс разделения кадра 802.11 на более мелкие кадры для последующей передачи называется фрагментацией; это помогает повысить надежность и снизить количество ошибок. В случаях, когда характеристики канала ограничивают доступность приема, передача меньшими (фрагментированными) кадрами увеличивает вероятность успешного проведения передачи.
Фрагментация выполняется на каждом передатчике непосредственно перед фактическим началом передачи. Процесс рекомбинации фрагментированных кадров в исходный нефрагментированный более длинный кадр называется дефрагментацией. Стандарт IEEE 802.11 определяет формат пакета для идентификации фрагментированных кадров для дефрагментации (показано на рисунке ниже).



Bytes	Байты
Frame Control	Управление кадром
Duration/ID	Продолжительность/Идентификатор
Address	Адрес
Sequence Control	Управление последовательностью

Frame Body	Тело кадра
Bits	Биты
Protocol Version	Версия протокола
Type	Тип
Subtype	Подтип
To DS	К DS
From DS	От DS
More Fragm	Большая фрагментация
Retry	Повторная попытка
Pwr Mgt	Управление мощностью
More Data	Больше данных
Rsvd	Зарезервировано
Fragment Number	Номер фрагмента
Sequence Number	Порядковый номер

Хотя фрагментация кадров способна обеспечить такие преимущества, как повышенная надежность и снижение вероятности ошибок при передаче по сети, эти преимущества могут быть достигнуты за счет общей пропускной способности сети, если не контролируются должным образом. Передача слишком большого количества мелких фрагментов по сети может указывать на то, что пользователи установили слишком низкий порог фрагментации кадра, в результате чего небольшие управляемые кадры фрагментируются в дополнение к более крупным кадрам. Поскольку этот процесс в конечном итоге приводит к передаче большего количества пакетов, в результате может пострадать производительность сети.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает статистику фрагментации в сети и предупреждает о злоупотреблении фрагментацией, которое может привести к снижению производительности сети WLAN. Необходимо тщательно установить порог фрагментации, чтобы сбалансировать получаемые преимущества и служебные данные. Обычно поставщики оборудования устанавливают порог фрагментации по умолчанию равным 1536.

Out of Order Fragmented Frames (Кадры, фрагментированные не по порядку)

Описание сигнала тревоги и возможные причины

Уровень MAC стандарта 802.11 поддерживает процессы фрагментации и дефрагментации. Процесс разделения кадра 802.11 на более мелкие кадры для последующей передачи называется фрагментацией; это помогает повысить надежность и снизить количество ошибок. В случаях, когда характеристики канала ограничивают доступность приема, передача меньшими (фрагментированными) кадрами увеличивает вероятность успешного выполнения передачи. Фрагментация выполняется на каждом передатчике непосредственно перед фактическим началом передачи. Процесс рекомбинации фрагментированных кадров в исходный нефрагментированный более длинный кадр называется дефрагментацией. Стандарт IEEE 802.11 определяет формат пакета для идентификации фрагментированных кадров для дефрагментации (показано на рисунке ниже).

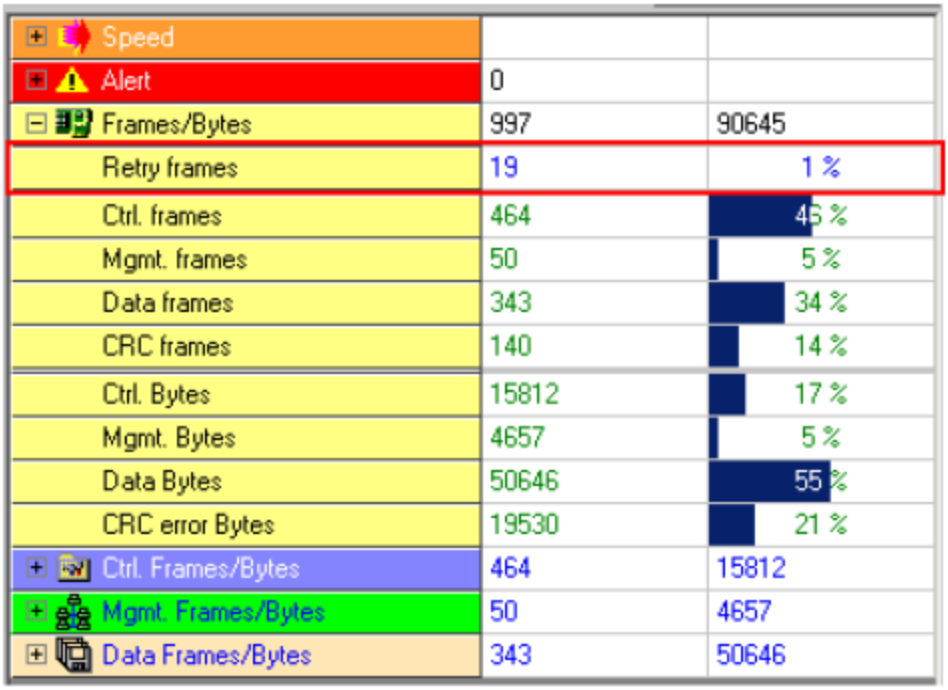
Bytes	Байты
Frame Control	Управление кадром
Duration/ID	Продолжительность/Идентификатор

Address	Адрес
Sequence Control	Управление последовательностью
Frame Body	Тело кадра
Bits	Биты
Protocol Version	Версия протокола
Type	Тип
Subtype	Подтип
To DS	К DS
From DS	От DS
More Fragm	Большая фрагментация
Retry	Повторная попытка
Pwr Mgt	Управление мощностью
More Data	Больше данных
Rsvd	Зарезервировано
Fragment Number	Номер фрагмента
Sequence Number	Порядковый номер

Как показано на рисунке выше, каждому фрагменту кадра назначается порядковый номер, который определяет порядок, в котором фрагменты будут переданы. Если кадры получены не по порядку, устройство-получатель должно передать кадр повтора, чтобы устройство-источник повторно отправило данные. Хотя в большинстве беспроводных сред будет наблюдаться определенный уровень трафика повторных попыток, большое количество повторно передаваемых кадров может привести к снижению пропускной способности и общей производительности сети.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает повторно передаваемые кадры и отслеживает их для каждого устройства и каждого канала. Смотрите рисунок ниже:

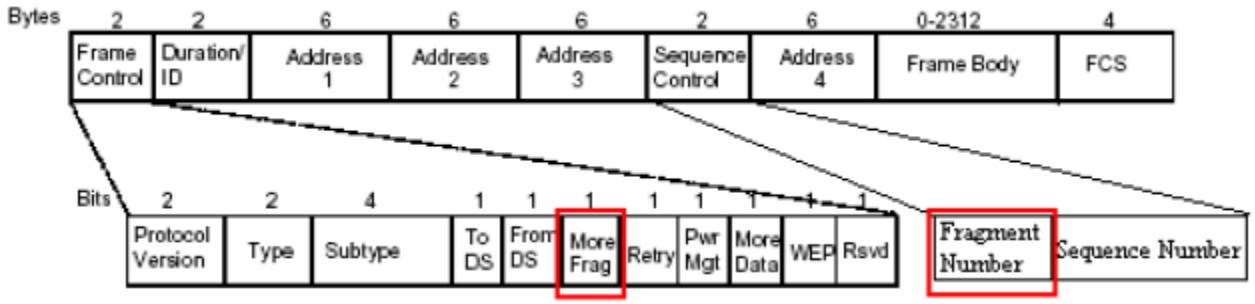


Высокий уровень повторной передачи кадров может быть вызван, среди прочего, сетевыми помехами, низким уровнем беспроводного сигнала (из-за недостаточной инфраструктуры) или скрытыми узлами. Для восстановления нормальной работы сети важно, чтобы сетевые администраторы устраняли основную причину, приводящую к повторной передаче кадров.

Incomplete or Invalid Fragmented Frames (Неполные или недопустимые фрагментированные кадры)

Описание сигнала тревоги и возможные причины

Уровень MAC стандарта 802.11 поддерживает процессы фрагментации и дефрагментации. Процесс разделения кадра 802.11 на более мелкие кадры для последующей передачи называется фрагментацией; это помогает повысить надежность и снизить количество ошибок. В случаях, когда характеристики канала ограничивают доступность приема, передача меньшими (фрагментированными) кадрами увеличивает вероятность успешной передачи. Фрагментация выполняется на каждом передатчике непосредственно перед фактическим началом передачи. Процесс рекомбинации фрагментированных кадров в исходный нефрагментированный более длинный кадр называется дефрагментацией. Стандарт IEEE 802.11 определяет формат пакета для идентификации фрагментированных кадров для дефрагментации (показано на рисунке ниже).

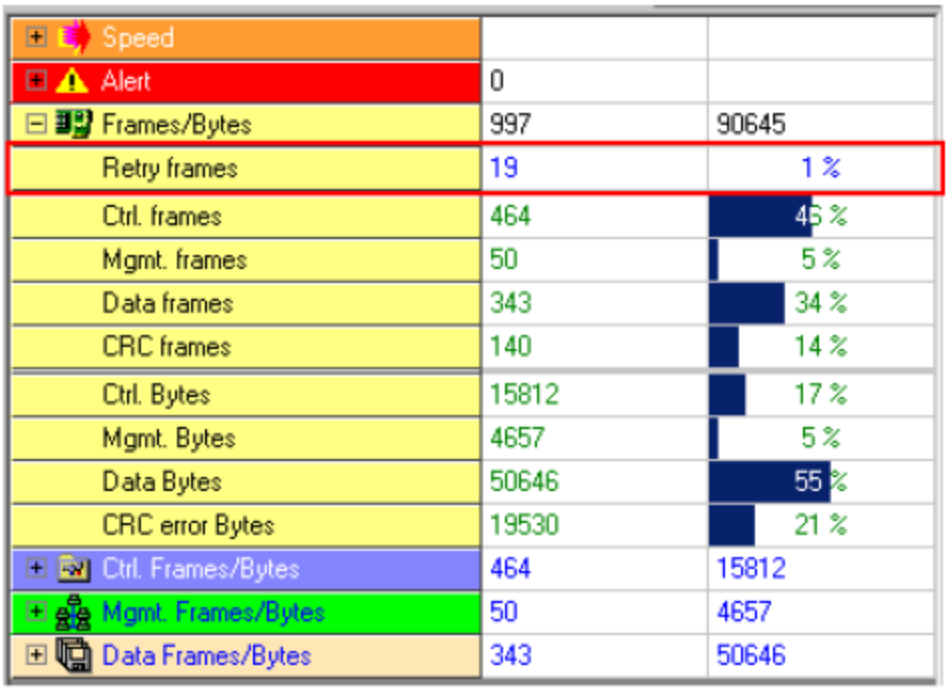


Bytes	Байты
Frame Control	Управление кадром
Duration/ID	Продолжительность/Идентификатор
Address	Адрес
Sequence Control	Управление последовательностью
Frame Body	Тело кадра
Bits	Биты
Protocol Version	Версия протокола
Type	Тип
Subtype	Подтип
To DS	К DS
From DS	От DS
More Fragm	Большая фрагментация
Retry	Повторная попытка
Pwr Mgt	Управление мощностью
More Data	Больше данных
Rsvd	Зарезервировано
Fragment Number	Номер фрагмента
Sequence Number	Порядковый номер

Если полученные кадры неполные или недопустимые, устройство-получатель должно передать кадр повтора, чтобы устройство-источник повторно отправило данные. Хотя в большинстве беспроводных сред будет наблюдаться определенный уровень трафика повторных попыток, большое количество повторно передаваемых кадров может привести к снижению пропускной способности и общей производительности сети.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает повторно передаваемые кадры и отслеживает их для каждого устройства и каждого канала. Смотрите рисунок ниже:



Speed		
Alert	0	
Frames/Bytes	997	90645
Retry frames	19	1 %
Ctrl. frames	464	45 %
Mgmt. frames	50	5 %
Data frames	343	34 %
CRC frames	140	14 %
Ctrl. Bytes	15812	17 %
Mgmt. Bytes	4657	5 %
Data Bytes	50646	55 %
CRC error Bytes	19530	21 %
Ctrl. Frames/Bytes	464	15812
Mgmt. Frames/Bytes	50	4657
Data Frames/Bytes	343	50646

Высокий уровень повторной передачи кадров может быть вызван, среди прочего, сетевыми помехами, низким уровнем беспроводного сигнала (из-за недостаточной инфраструктуры) или скрытыми узлами. Для восстановления нормальной работы сети важно, чтобы сетевые администраторы устраняли основную причину, приводящую к повторной передаче кадров.

Denial-of-Service Attack: Beacon Flood (Атака типа «отказ в обслуживании»: Флуд кадров маяка)

Описание сигнала тревоги и возможные причины

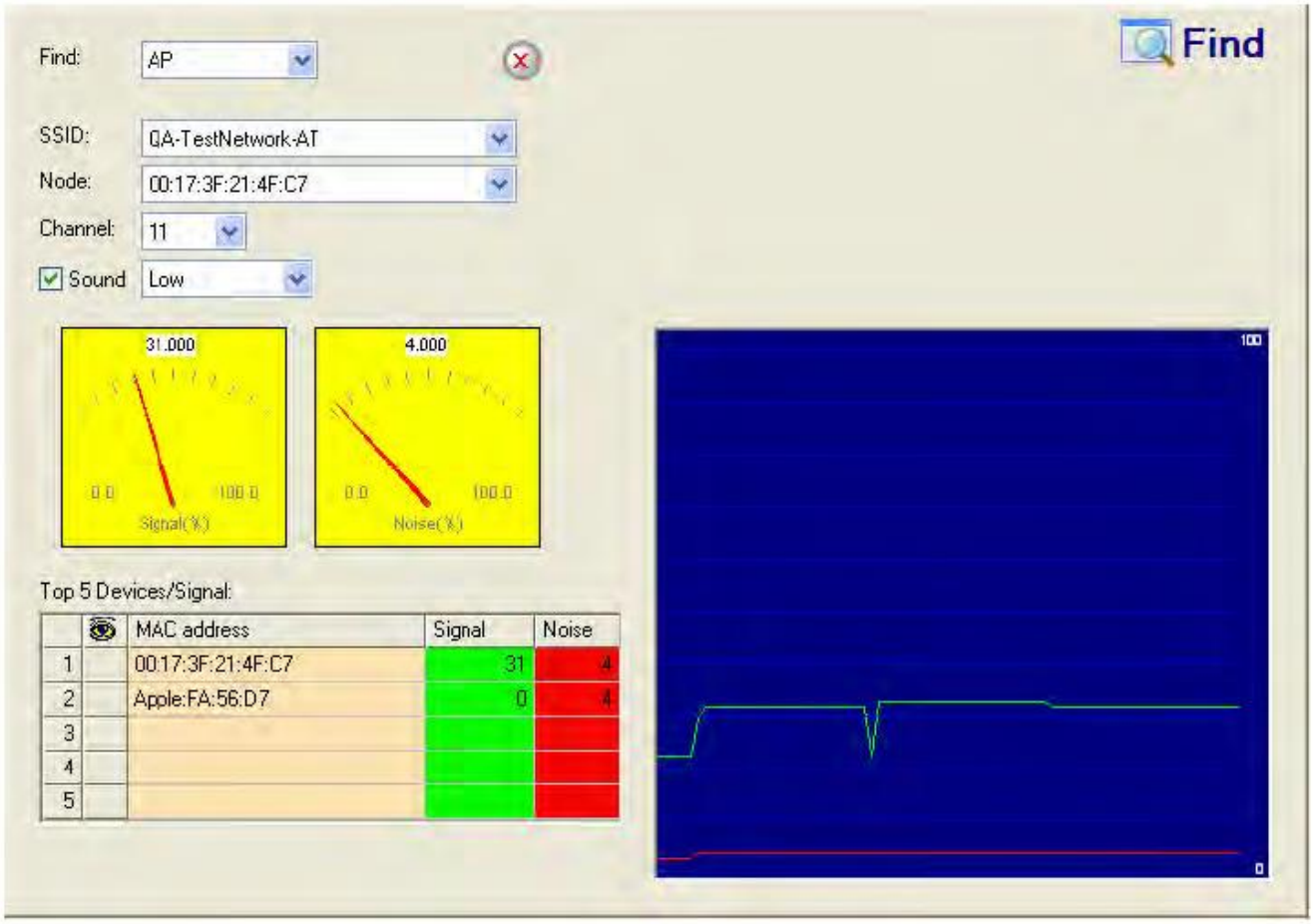
Для уведомления локальных устройств о конфигурации сети точки доступа в корпоративной беспроводной сети постоянно транслируют кадры маяка. Эти кадры могут содержать различные данные, включая метку времени, SSID, механизм аутентификации и скорости передачи данных, поддерживаемые точкой доступа. После приема кадра маяка станции смогут использовать предоставленную информацию для установления связи с точкой доступа.

Обычно перед попыткой подключения к точке доступа беспроводным станциям требуется кадр маяка, который позволит предоставить соответствующие учетные данные для аутентификации. Это представляет собой потенциальную уязвимость, поскольку, если станция не сможет получить желаемый кадр маяка, то не сможет и подключиться к точке доступа. Из-за того, что все точки доступа в сети будут передавать кадры маяка через равные промежутки времени, в особо загроможденной среде у станций могут возникать трудности с выбором соответствующего кадра маяка.

Злоумышленник может воспользоваться этой уязвимостью для того, чтобы легитимные корпоративные станции не смогли подключаться к беспроводной сети. Чтобы инициировать атаку типа «отказ в обслуживании», злоумышленник может заполнить беспроводную среду случайными кадрами маяка, которые содержат поддельный MAC-адрес и данные SSID. Слишком большое количество сигналов маяка в эфире может помешать станциям принимать сигналы маяка от авторизованных точек доступа сети, что воспрепятствует установлению станциями беспроводного доступа.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает уровень обнаруженных кадров маяков и инициирует сигнал тревоги Beacon Flood при превышении порогового значения. Даже в тех случаях, когда сигналы маяка являются достоверными (например, из-за особенно плотного развертывания точек доступа), объем их кадров может снижать общую пропускную способность сети. Следовательно, источник (или источники) ошибочных кадров следует обнаружить с помощью инструмента Find (Найти), после чего его можно будет удалить из корпоративной среды.



Denial-of-Service Attack: MDK3 Destruction Attack (Атака типа «отказ в обслуживании»: Атака MDK3 Destruction)

Описание сигнала тревоги и возможные причины

MDK3 - это набор инструментов для взлома, который позволяет пользователям использовать ряд различных методов проникновения в систему безопасности, направленных против целевой корпоративной точки доступа. Режим MDK3-Destruction - это конкретная реализация пакета, в котором используется набор инструментов для полного отключения атакуемой точки доступа. Во время атаки MDK3-Destruction инструмент одновременно:

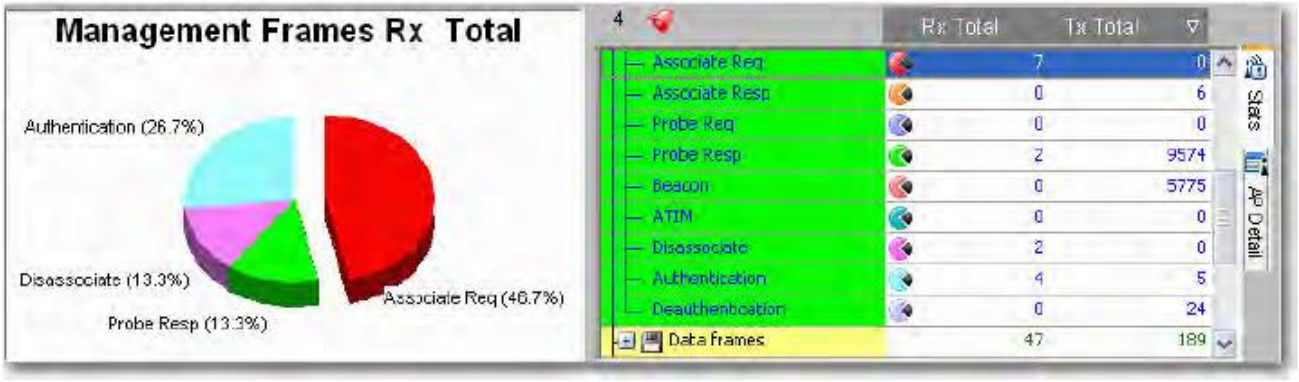
- Инициирует атаку с помощью лавинной передачи (флуда) кадров маяка, создавая в беспроводной среде несколько поддельных точек доступа,
- Запускает лавинную атаку аутентификации против целевой точки доступа, не позволяя ей обслуживать клиентов, и
- Запускает лавинную атаку деаутентификации против целевой точки доступа, разрывая все активные соединения легитимных клиентов.

Пока продолжается атака, пользователи не смогут получить доступ к целевой точке доступа. Аутентифицированные клиенты, которые были отключены от точки доступа из-за лавинной атаки деаутентификации, могут попытаться установить связь с созданными поддельными точками доступа, что способно привести к отправке корпоративных данных злоумышленнику.

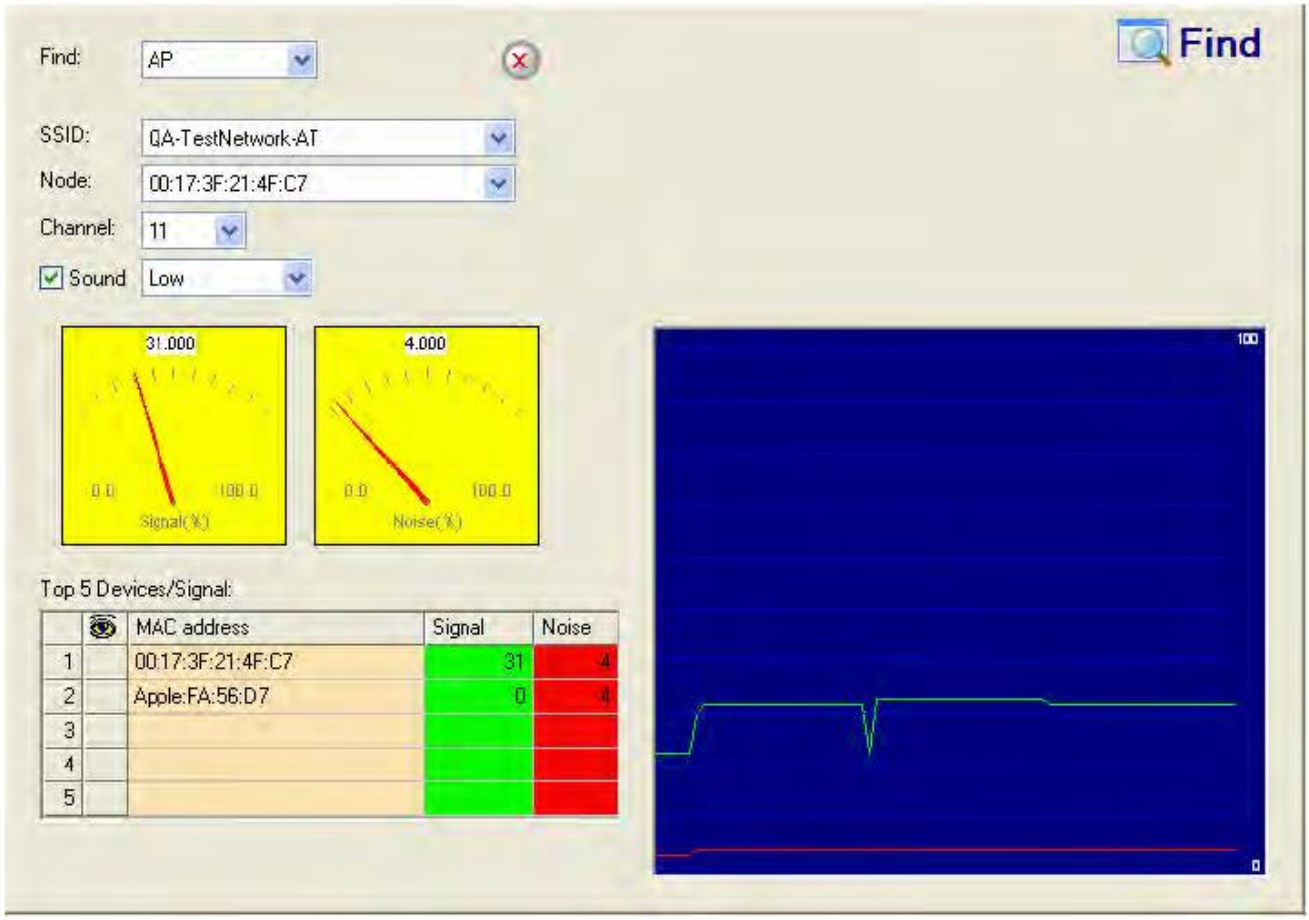
Из-за объема передаваемого трафика после остановки атаки может потребоваться перезагрузить целевую точку доступа. Дополнительные сведения об инструментах MDK3 смотрите на веб-странице http://homepages.tu-darmstadt.de/~p_larbig/wlan/.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает симптомы атаки MDK3-Destruction и при их обнаружении выдает сигнал тревоги. Из-за значительного воздействия, которое эта атака может оказать на беспроводную сеть, настоятельно рекомендуется как можно скорее определить ее источник с помощью экрана Infrastructure (Инфраструктура).



После того, как устройство идентифицировано, воспользуйтесь инструментом Find (Найти) для определения его местонахождения. ИТ-персонал должен немедленно удалить устройство, прежде чем будет нанесен дополнительный ущерб. Кроме того, в некоторых сетях может потребоваться перезагрузить затронутые корпоративные точки доступа, чтобы перед возобновлением работы беспроводной сети очистить их таблицы подключения.



KARMA Tool Detected (Обнаружен инструмент KARMA)

Описание сигнала тревоги и возможные причины

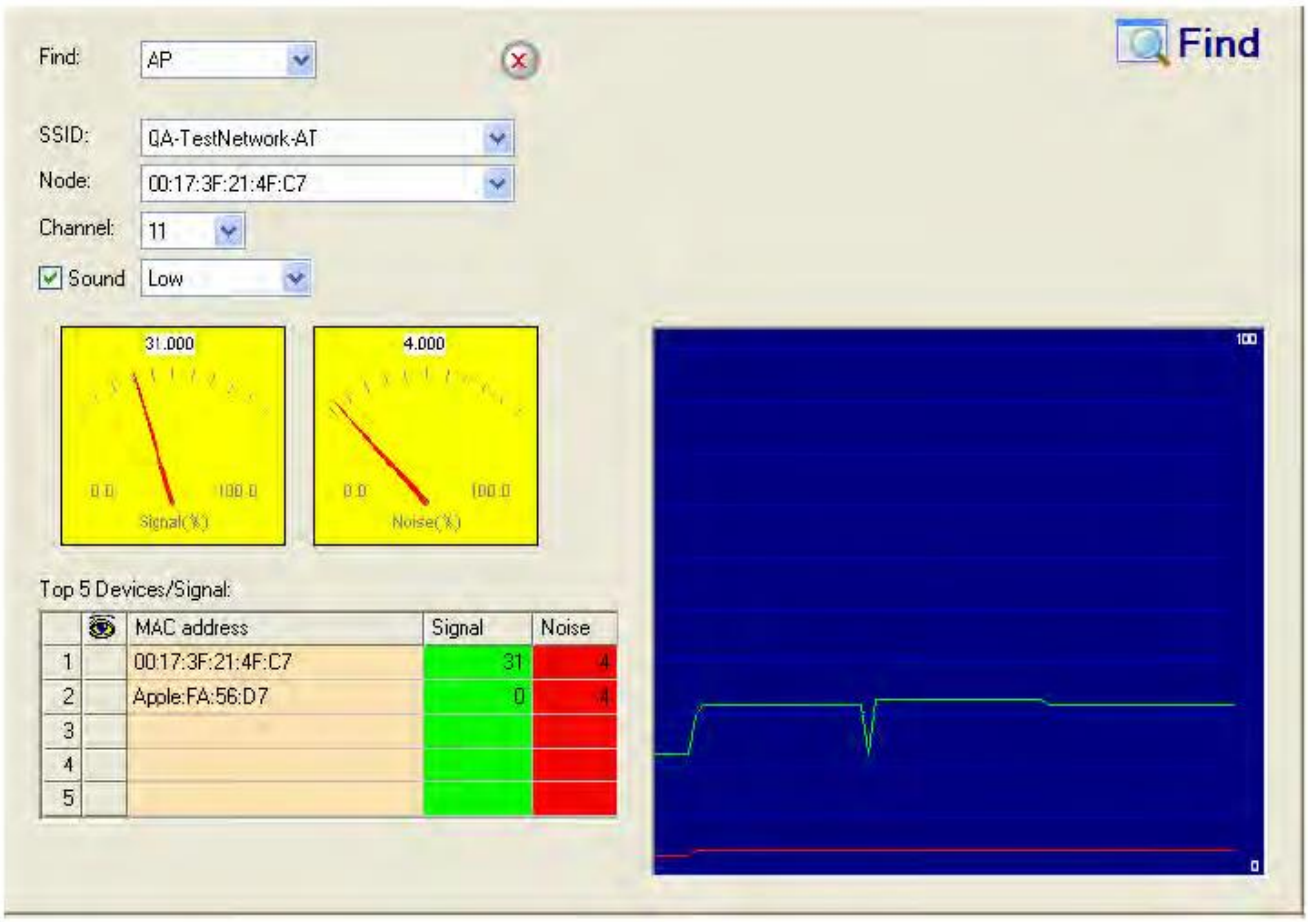
KARMA - это набор беспроводных инструментов, предназначенных для проверки безопасности беспроводной сети. Базовая реализация набора инструментов позволяет злоумышленнику отслеживать кадры зондирующего запроса, передаваемые станциями, ищущими известные беспроводные идентификаторы SSID. Затем, используя один из захваченных SSID, злоумышленник может создать неавторизованную точку доступа, что способно привести к автоматическому подключению к ней корпоративной станции. Более продвинутые злоумышленники могут воспользоваться этим подключением для получения учетных данных корпоративной аутентификации или атаковать саму клиентскую станцию.

Обновления набора инструментов KARMA оптимизируют процесс атаки, позволяя пользователю настроить неавторизованную точку доступа, которая будет реагировать на любые обнаруженные кадры зондирующего запроса. Например, если два клиента ищут два разных идентификатора SSID (например, «home» для первого и «corporate» для второго), мошенническая точка доступа ответит каждому как «home» и «corporate» по очереди. Таким образом, злоумышленник может использовать соединения нескольких клиентов в сети вместо того, чтобы требовать их подключения по очереди. После установления соединения оба пользователя рискуют передать через атакующую точку доступа конфиденциальную информацию.

Для получения дополнительной информации о KARMA посетите http://blog.trailofbits.com/karma/.

Решение AirMagnet

В некоторых случаях ИТ-персонал использует инструменты KARMA, чтобы гарантировать соответствие корпоративных клиентов действующим корпоративным политикам беспроводной связи. Если с помощью инструментов KARMA обнаруживается неизвестное или неавторизованное устройство, пользователи должны определить источник кадров с помощью инструмента Find (Найти) и удалить его из беспроводной среды.



Чтобы гарантировать защиту беспроводных клиентов компании от подобных атак, пользователям рекомендуется настроить подключение своих станций к сетям не автоматически, а только по запросу. Это не позволит инструментам KARMA перехватывать зондирующие запросы и легко эмулировать корпоративные точки доступа.

Wi-FiTap Tool Detected (Обнаружен инструмент Wi-FiTap)

Описание сигнала тревоги и возможные причины

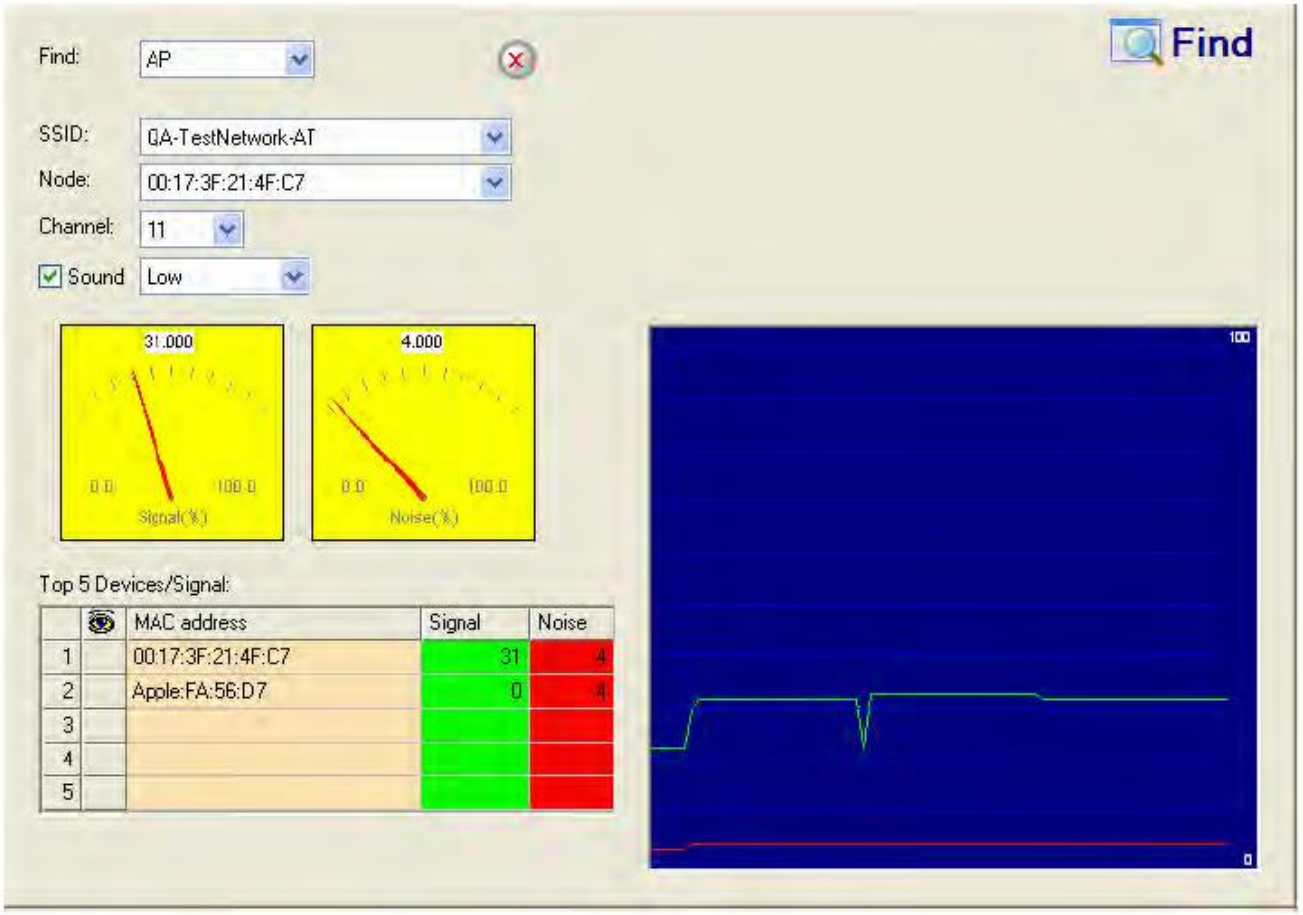
Wi-FiTap - это инструмент, который позволяет атакующей станции напрямую связываться с целевым клиентом, не подключаясь к корпоративной беспроводной сети. Избегая необходимости подключаться к корпоративной точке доступа, злоумышленник эффективно обходит любые меры безопасности, настроенные для защиты корпоративной сети (например, Cisco PSPF). После успешного установления соединения с легитимным клиентом утилиту Wi-FiTap можно изменить, чтобы позволить злоумышленнику впоследствии эмулировать корпоративную точку доступа, отправляя поддельные ответы на захваченные передачи целевой станции. Так злоумышленник сможет отслеживать трафик критических или защищенных данных, представляя угрозу безопасности.

Во время атаки Wi-FiTap мошенническая станция сначала отслеживает беспроводное пространство, чтобы определить каналы (канал), по которым осуществляют передачу корпоративные точки доступа. После определения целевой точки доступа и канала злоумышленник настраивает инструмент Wi-FiTap для эмуляции BSSID точки доступа (например, MAC-адреса) и настраивает беспроводную карту атакующей машины для эмуляции точки доступа. После получения списка сетевых клиентов авторизованной точки доступа (с помощью такой утилиты, как Tcpdump или Ethereal) злоумышленник может напрямую взаимодействовать с любым из этих клиентов, представляясь легитимной точкой доступа.

Для получения дополнительной информации об инструменте Wi-FiTap смотрите Http://sid.rstack.org/index.php/Wi-Fitap_EN.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает беспроводной трафик на предмет потенциальных экземпляров утилиты Wi-FiTap и при обнаружении атаки уведомляет пользователей. Персоналу службы безопасности рекомендуется идентифицировать устройство и определить его местонахождение с помощью инструмента Find (Найти). Чтобы предотвратить перехват конфиденциальных передач, атакующую станцию следует как можно скорее удалить из беспроводной среды.



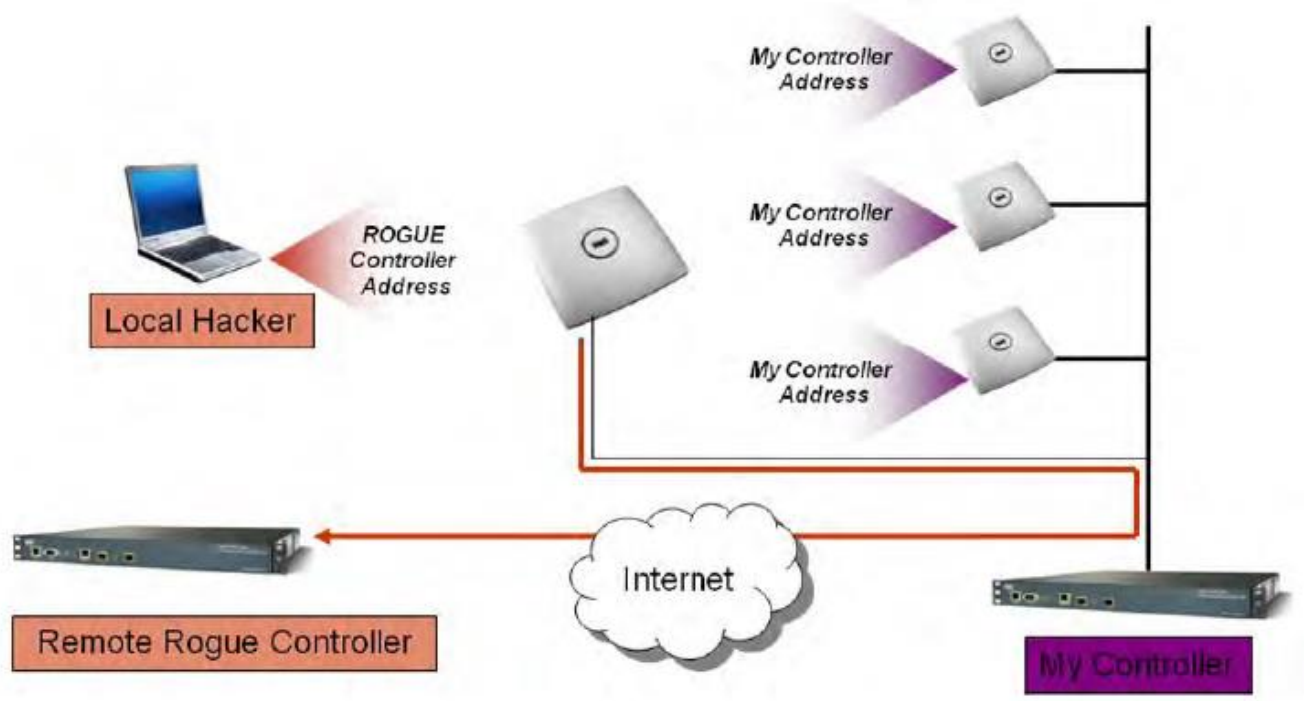
SkyJack Attack Detected (Обнаружена атака SkyJack)

Описание сигнала тревоги и возможные причины

По мере роста популярности облегченных точек доступа, управляемых централизованными системами, растет и потребность в простом развертывании по принципу plug-and-play и резервном аварийном переключении этих точек доступа и систем управления. Корпоративная беспроводная сеть перестает быть признаком роскоши и становится всё более важным элементом сетевой инфраструктуры, поскольку простота ее развертывания и настройки резервирования способствуют росту ее использования ИТ-командами, желающими быстро предоставить сотрудникам доступ к сети. Многие производители беспроводной инфраструктуры пошли на удовлетворение этих отраслевых требований, позволив облегченной точке доступа автоматически обнаруживать системы управления. Это помогает вновь развернутым точкам доступа впервые найти систему управления, а уже развернутым точкам доступа переключаться на резервные системы управления, если их основная система управления отключается. Методы, с помощью которых точки доступа находят систему управления, включают полученную информацию в ответе DHCP, настроенные на заводе записи DNS, широковещательные сообщения обнаружения на своих проводных интерфейсах и прослушивание определенных кадров от других, уже настроенных инфраструктурных точек доступа на своих беспроводных интерфейсах. К сожалению, именно последний метод представляет серьезную угрозу безопасности компаний, использующих облегченные точки доступа для развертывания централизованной системы управления.

Кадры, используемые для помощи недавно развернутым или аварийным точкам доступа, зачастую представляют собой незашифрованные кадры данных, отправляемые от уже развернутых точек доступа, независимо от шифрования и аутентификации, которые используются этими уже развернутыми точками доступа. Необходимость в этом возникает из-за того, что недавно развернутые или аварийные точки доступа могут не иметь правильных ключей шифрования для расшифровки кадров, которые нужны для беспрепятственного развертывания или аварийного переключения. Однако точки доступа к инфраструктуре, прослушивающие и обрабатывающие данные в незашифрованных кадрах, представляют серьезную угрозу безопасности. Эти кадры могут включать IP-адреса и MAC-адреса систем управления, а также другую необходимую для надлежащего управления точкой доступа информацию. Подменяя эти незашифрованные кадры и передавая их в неконтролируемую беспроводную среду, злоумышленник может обмануть недавно развернутую или аварийную точку доступа и вынудить ее

подключиться к системе управления по своему выбору, включая внешнюю систему, находящуюся под его контролем. Как только точка доступа сетевой инфраструктуры подключится к системе управления злоумышленника, она фактически перейдет в режим SkyJacked, и злоумышленник сможет заставить точку доступа работать любым способом. Злоумышленник может использовать открытое беспроводное соединение для получения доступа к корпоративной проводной сети или попытаться получить данные для входа в систему от корпоративных клиентов, пытающихся подключиться к контролируемой им точке доступа.



My Controller Address	Адрес моего контроллера
ROGUE Controller Address	Адрес мошеннического контроллера
Local Hacker	Локальный хакер
Internet	Интернет
Remote Rogue Controller	Удаленный мошеннический контроллер
My Controller	Мой контроллер

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer предупреждает пользователя о шаблонах беспроводного трафика, которые соответствуют сигнатурам потенциальных попыток атаки SkyJack. Если подается подобное предупреждение, пользователи должны внимательно контролировать точки доступа и системы управления своей инфраструктурой, чтобы убедиться в их ожидаемом рабочем состоянии. Дополнительная защита от атак SkyJack включает отключение помощи при развертывании и аварийном переключении в беспроводной среде.

Rogue Station by MAC Address (ACL) (Мошенническая станция по MAC-адресу (ACL))

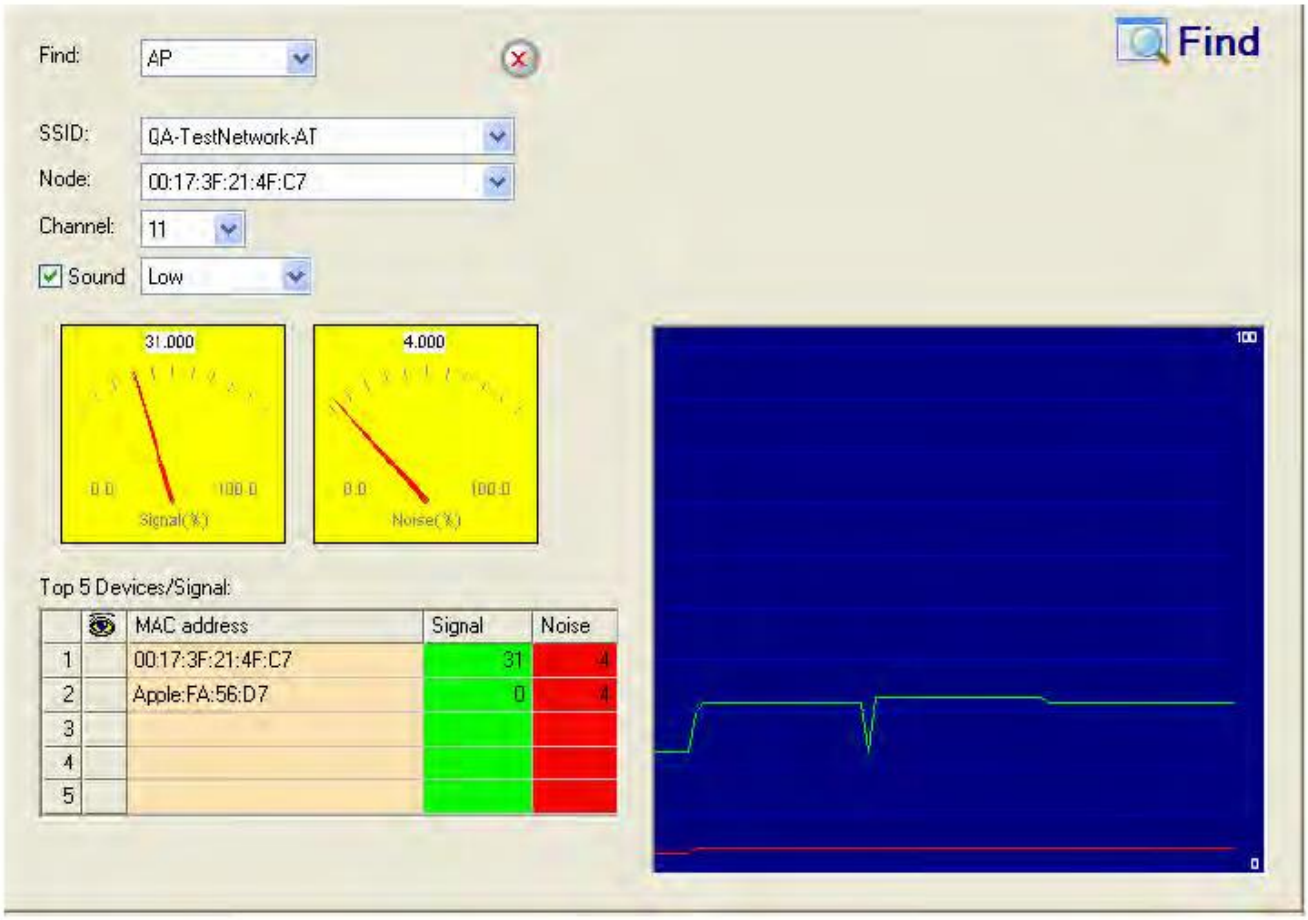
Описание сигнала тревоги и возможные причины

После настройки списка MAC-адресов авторизованных клиентских станций вашего предприятия приложение AirMagnet Wi-Fi Analyzer сможет предупреждать администраторов WLAN о неавторизованных (мошеннических) станциях, MAC-адрес которых не входит в предварительно настроенный список адресов. Список авторизованных MAC-адресов можно импортировать в приложение AirMagnet Enterprise из файла (AccessControl.txt). Этот файл является общим для точек доступа, станций сетевой инфраструктуры и устройств Ad-hoc. Его также можно генерировать автоматически, запросив приложение AirMagnet Enterprise принять все или определенное подмножество существующих точек доступа, обнаруженных датчиками AirMagnet SmartEdge.

Неавторизованные станции, установленные неавторизованными сотрудниками, обычно не соответствуют стандартным корпоративным методам развертывания и могут поставить под угрозу безопасность как беспроводной, так и проводной сети. Сигнал тревоги Rogue Station может также указывать на попытки злоумышленников взломать проводную сеть предприятия. Следует тщательно изучать обнаруженные приложением AirMagnet Wi-Fi Analyzer неавторизованные устройства.

Решение AirMagnet

После обнаружения неавторизованной станции и сообщения об этом от приложения AirMagnet WiFi Analyzer администратор WLAN может использовать инструмент FIND (Найти) для определения местонахождения неавторизованного устройства.

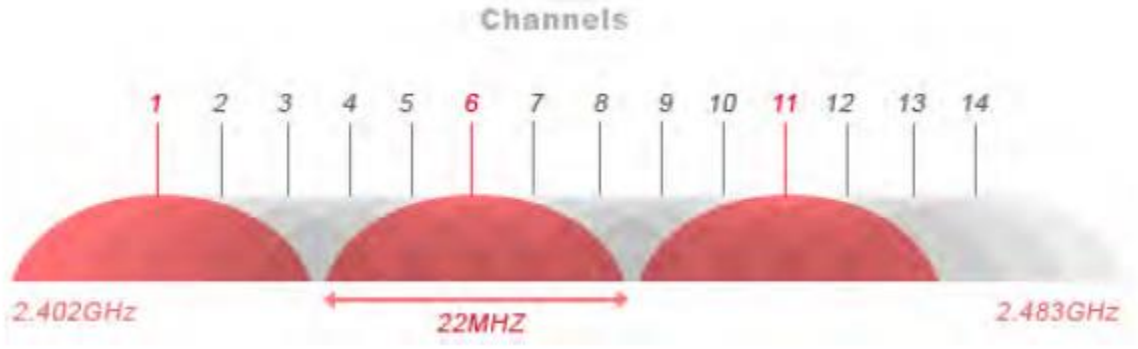


Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Interfering APs Detected (Обнаружены создающие помехи точки доступа)

Описание сигнала тревоги и возможные причины

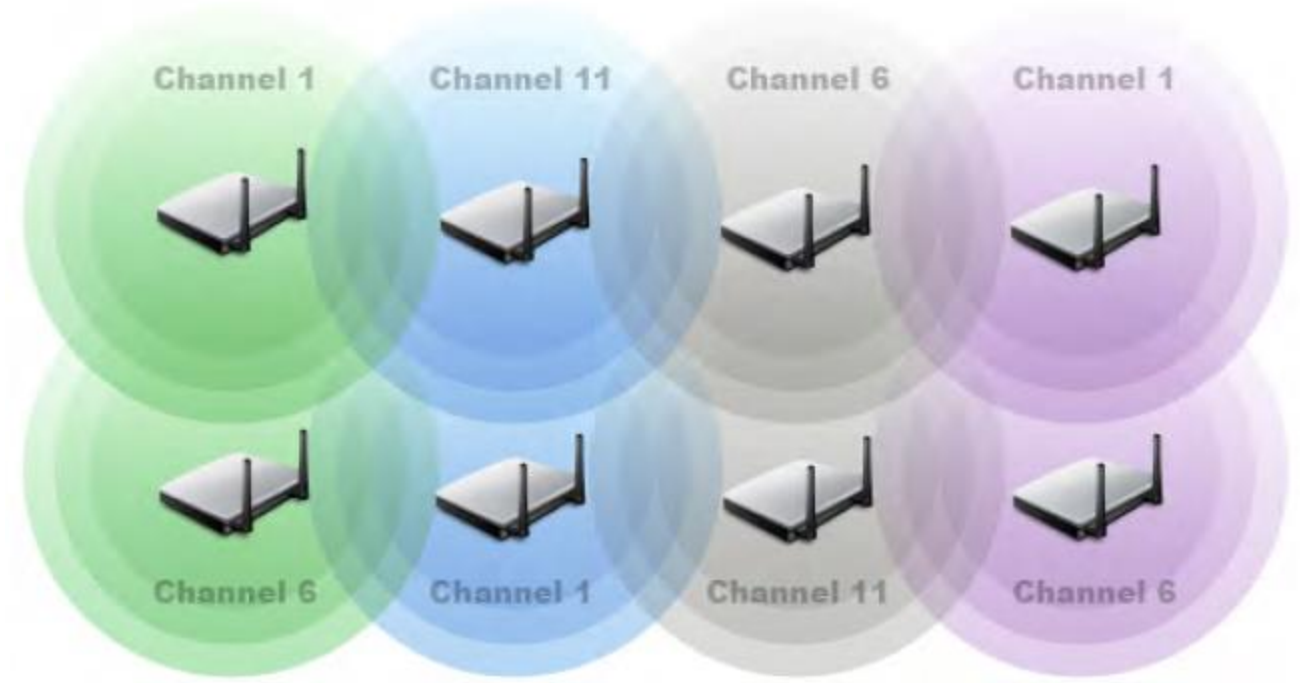
Устройства 802.11b и 11g работают в радиочастотном диапазоне 2,4 ГГц. В этом диапазоне частот стандартом IEEE заданы в общей сложности 14 каналов, каждый из которых занимает 22 МГц. Соседние каналы перекрываются друг с другом в радиочастотном спектре (смотрите рисунок ниже).



Channels	Каналы
2.402 GHz	2,402 ГГц
22 MHz	22 МГц
2.483 GHz	2,483 ГГц

Распределение каналов и перекрывание частот для 802.11b и 11g

Используемые беспроводными устройствами, работающими в соседних каналах (номера каналов различаются меньше, чем на 5), радиочастотные полосы перекрываются, и они создают помехи друг другу. В идеальном случае во избежание подобных проблем точки доступа должны отстоять друг от друга на 5 каналов. На рисунке ниже приводится пример распределения каналов и развертывания точки доступа.

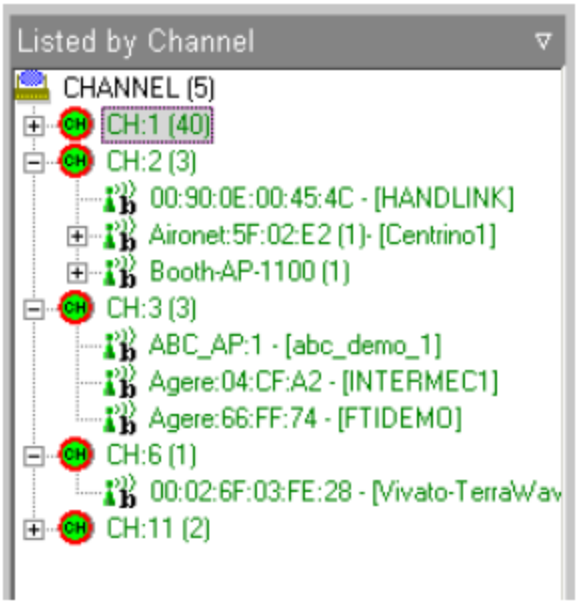


Channel	Канал

Обследование площадки для выделения неперекрывающихся каналов физически смежным точкам доступа

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer анализирует распределение и использование каналов для обнаружения их взаимных помех. Сигнал тревоги подается, когда полоса частот канала перекрывается более чем допустимым числом точек доступа (настраиваемый пользователем порог подачи сигнала тревоги). Например, если приложение AirMagnet WiFi Analyzer обнаруживает 5 точек доступа, работающих в каналах 1, 2, 3, 4, 5 и 6 по отдельности, то сформирует этот сигнал тревоги, чтобы указать, что все эти точки доступа мешают друг другу, а количество точек доступа, использующих перекрывающиеся частоты, превышает пороговое значение по умолчанию, равное 3. Большинство экспертов советуют использовать каналы 1, 6 и 11, а некоторые рекомендуют использовать только каналы 1 и 11. Для дальнейшего изучения текущего использования каналов и принятия необходимых мер пользователь может использовать экран AirMagnet Infrastructure.



На экране AirMagnet Infrastructure (список по каналам) отображается распределение каналов

Policy – Mismatched SSID (Политика - Несоответствующий идентификатор SSID)

Определенный клиент настроен с идентификатором SSID, который не соответствует ни одному из доступных SSID в этой беспроводной локальной сети.

Policy – Client with match-all SSID (Политика - Клиент с универсальным идентификатором SSID)

Определенный клиент настроен с универсальным идентификатором SSID (нулевая последовательность или ANY (ЛЮБОЙ)), который не принимается ни одной точкой доступа в этой беспроводной локальной сети, поскольку они принимают только конкретные идентификаторы SSID.

Policy – Mismatched RF Channel (Политика - Несоответствующий радиочастотный канал)

Определенный радиочастотный канал не имеет клиентов, вместо этого имеются точки доступа с совпадающим идентификатором SSID, что может быть вызвано неправильной конфигурацией клиентов.

Policy – Mismatched privacy setting (Политика - Несоответствие настроек конфиденциальности)

Определенные клиенты и точки доступа не могут связаться друг с другом из-за несоответствующей конфигурации шифрования WEP.

Conflicting AP Configuration (Конфликтная конфигурация точки доступа)

Описание сигнала тревоги и возможные причины

Одним из способов проверки приложением AirMagnet WiFi Analyzer политики конфигурации является проверка согласованности конфигурации точек доступа, поддерживающих один и тот же идентификатор SSID. Крупные корпорации будут иметь большие беспроводные сети с более чем одной точкой доступа, обеспечивающей доступ к беспроводным услугам. Для эффективного роуминга клиентов важно, чтобы точки доступа с одинаковыми идентификаторами SSID имели аналогичные конфигурации. Приведенные ниже параметры конфигурации должны иметь одинаковые настройки для всех точек доступа с одним и тем же идентификатором SSID:

- Аутентификация и шифрование (статический WEP, TKIP и т.д.)
- Рабочие параметры (короткая/длинная преамбула)
- Широковещательный SSID

Несогласованность настройки точек доступа может привести к несогласованному обеспечению безопасности или несогласованному взаимодействию клиентов.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer определяет точки доступа с несоответствующей конфигурацией, чтобы администратор WLAN мог её исправить. Примите соответствующие меры для обеспечения согласованных конфигураций во всей беспроводной среде. Сюда входит обеспечение одинаковых настроек шифрования и параметров преамбулы.

Policy – Authentication failure (Политика - Ошибка аутентификации)

Ошибка аутентификации

Policy – (Re)Association failure (Политика – Ошибка повторного подключения)

Ошибка повторного подключения.

Policy – Possible equipment failure (Политика - Возможный отказ оборудования)

Возможный отказ оборудования.

AP Using Non-standard SSID (Точка доступа с нестандартным идентификатором SSID)

Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer предупреждает администратора WLAN о точках доступа в ACL (in-ACL Access Points), которые не используют стандартные идентификаторы SSID. Например, если развернутая сеть WLAN настроена только с идентификаторами MyOfficeWlan и MyVoIPWlan, эти два SSID необходимо затем включить в авторизованный список SSID Group (Группа SSID). После импортирования этого списка приложение AirMagnet WiFi Analyzer выдает сигнал тревоги «AP Using Non-standard SSID», если обнаруживается точка доступа, помеченная in-ACL и работающая с другим идентификатором SSID. Внезапные изменения идентификатора SSID точки доступа могут указывать на то, что к ней получило

доступ неавторизованное лицо, которое и внесло эти изменения. Любые изменения SSID могут вызвать прерывание работы в сети для ваших клиентов, поскольку они больше не обнаруживают исходный идентификатор SSID, настроенный в их утилите клиента или нулевой конфигурации Windows.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer также предупреждает пользователя о любых внезапных изменениях идентификаторов SSID точек доступа в списке ACL. Это может указывать, что злоумышленник контролирует точку доступа и внес изменение в конфигурацию SSID. Это может привести к отключению всех авторизованных клиентов от точки доступа, поскольку теперь они не находятся в одной сети, или может поставить под угрозу безопасность сети. Чтобы продолжить предоставление услуг клиентам, подключитесь к точке доступа, конфигурация которой изменилась, назначьте более надежный пароль для входа в точку доступа и измените идентификацию SSID обратно на исходную.

Policy – AP signal out of range (Политика - Сигнал точки доступа вне радиуса действия)

Сигнал точки доступа вне радиуса действия.

Policy – Mismatched capability settings (Политика – Несогласованные настройки возможностей)

Несогласованные настройки возможностей.

Policy – Device with bad WEP key (Политика - Устройство с плохим ключом WEP)

Устройство с плохим ключом WEP.

Channel With High Noise Level (Канал с высоким уровнем шума)

Описание сигнала тревоги и возможные причины

Появление беспроводных технологий означает, что несколько разных беспроводных устройств будут работать в непосредственной близости друг от друга. В нелицензируемом диапазоне частот 2,4 ГГц устройства 802.11b и 11g - не единственное работающее беспроводное оборудование. Другие технологии, включая Bluetooth, беспроводные телефоны диапазона 2,4 ГГц, беспроводные камеры систем видеонаблюдения, микроволновые печи, радионяни, используемые в больницах, и т.п. могут создавать помехи сетям WLAN, что приводит к увеличению BER (коэффициент битовых ошибок), и, следовательно, к уменьшению покрытия и снижению производительности. В диапазоне частот 5 ГГц, который использует стандарт 802.11a, нормативные правила были более строгими в пользу сетей передачи данных WLAN; наличие шума возможно, но не в той степени, как в спектре 2,4 ГГц, поэтому возникает меньше проблем с помехами.

Уровень шумов	Влияние на рабочее расстояние в помещении	Влияние на рабочее расстояние вне помещения
0 дБ	0%	0%
3 дБ	19%	30%
5 дБ	30%	44%
10 дБ	50%	68%

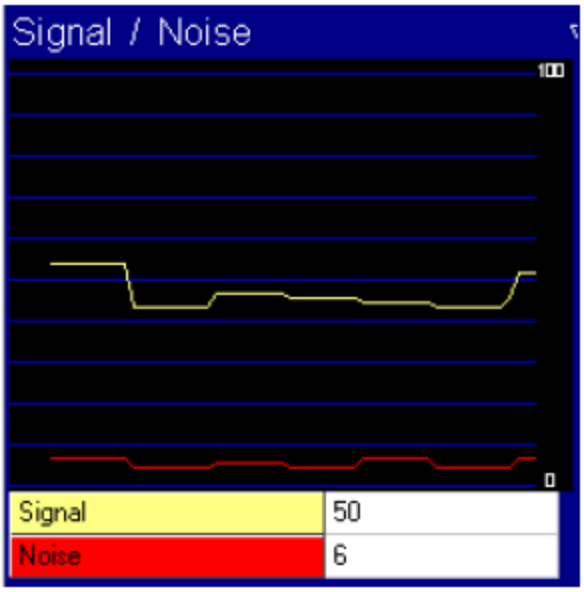
Воздействие радиочастотных шумов на рабочие расстояние беспроводного устройства

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer не способно (без дополнительной помощи, о чем смотрите ниже) различать такие источники помех, как Bluetooth, микроволновая печь, телефоны и т.п., и их присутствие отображается в приложении AirMagnet WiFi Analyzer в виде шумов радиочастотного канала. Отслеживая уровень шумов для каждого канала, приложение AirMagnet WiFi Analyzer выдает данный сигнал тревоги для канала, который имеет устойчиво высокий уровень шумов. Чтобы дополнительно идентифицировать источник шумов в канале, можно использовать отслеживание с помощью направленной антенны. По мере приближения к источнику уровень шумов будет усиливаться. Как только источник будет обнаружен, с ним следует немедленно разбираться.

Приобретение приложения AirMagnet Spectrum Analyzer и его интегрирование с приложением с AirMagnet WiFi Analyzer даст вам еще более мощный инструмент, который позволит идентифицировать дополнительные источники помех. Включив функцию интеграции анализатора спектра, вы сможете использовать страницу RF Interference (Радиочастотные помехи), чтобы определить, какие каналы испытывают помехи от источников, отличных от 802.11. Затем с помощью инструмента Find (Найти) можно будет отследить эти устройства и устранить проблему.

Если вызывающее проблемы оборудование принадлежит вашей компании, всё можно будет легко исправить, но если оно принадлежит соседней компании, исправление ситуации может оказаться гораздо более сложной задачей. Это подчеркивает важность эффективного обследования площадки перед началом развертывания корпоративной сети WLAN, что позволит лучше изучить окружение и получить более высокие конечные результаты.



Уровень шумов канала, доступный на удаленном анализаторе

Excessive Multicast/Broadcast on Channel (Чрезмерная многоадресная/широковещательная передача на канале)

Описание сигнала тревоги и возможные причины

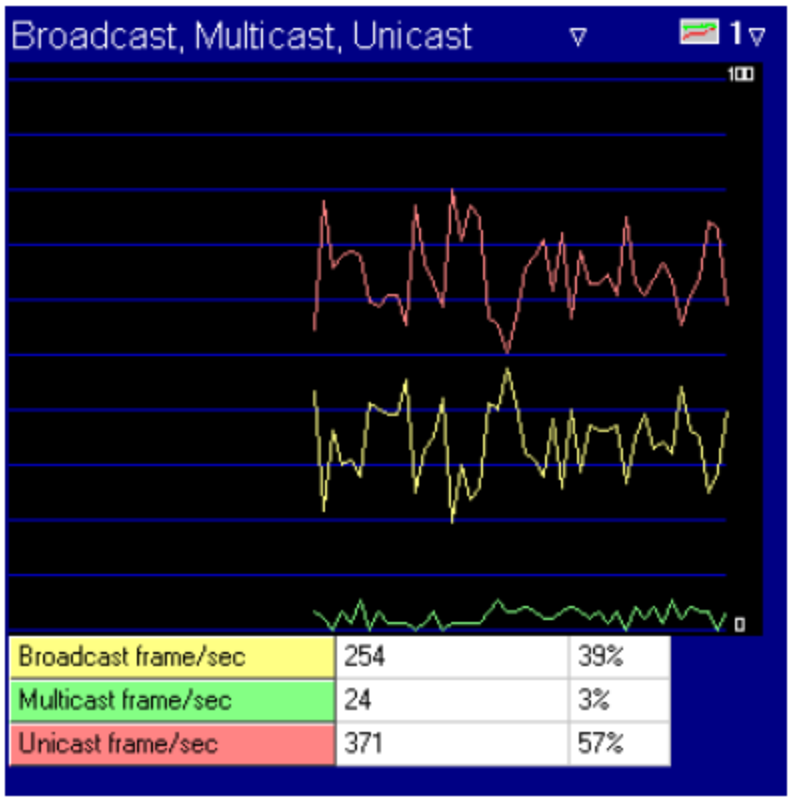
Подобно проводной сети, чрезмерное количество широковещательных и многоадресных кадров создает дополнительную нагрузку на все устройства в проводной локальной сети. Более чувствительной сеть WLAN к многоадресным и широковещательным кадрам по сравнению с проводными сетями делает тот факт, что все многоадресные и широковещательные кадры передаются с низкой скоростью (например, 1 или 2 Мбит/с для WLAN 802.11b). Такие низкоскоростные передачи потребляют большую полосу пропускания сети WLAN.

Помимо неэффективного использования полосы пропускания низкоскоростные многоадресные и широковещательные кадры требуют большего времени для выполнения процесса передачи, что приводит к более высоким задержкам для других устройств, ожидающих освобождения беспроводной среды. Чрезмерное количество многоадресных и широковещательных кадров вызывает джиттер в таких

чувствительных к задержке приложениях WLAN, как VoIP. Например, передача 1000-байтового кадра широковещательной передачи со скоростью 1 Мбит/с займет не менее 8 миллисекунд, что является значительной задержкой для голосового приложения.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает использование многоадресных и широковещательных кадров для каждого канала и устройства, чтобы сообщить о злоупотреблениях. Порог срабатывания сигнализации - это процентное отношение многоадресных и широковещательных кадров к общему количеству кадров по устройству или каналу. Для дальнейшего изучения ситуации с многоадресной и широковещательной рассылкой можно использовать показанный ниже экран Channel (Канал) или Infrastructure (Инфраструктура), на котором отображается соответствующая статистика.



Кадры многоадресной и широковещательной передачи для возникновения сигнала тревоги о неправильном использовании

Spoofed MAC Address Detected (Обнаружен поддельный MAC-адрес)

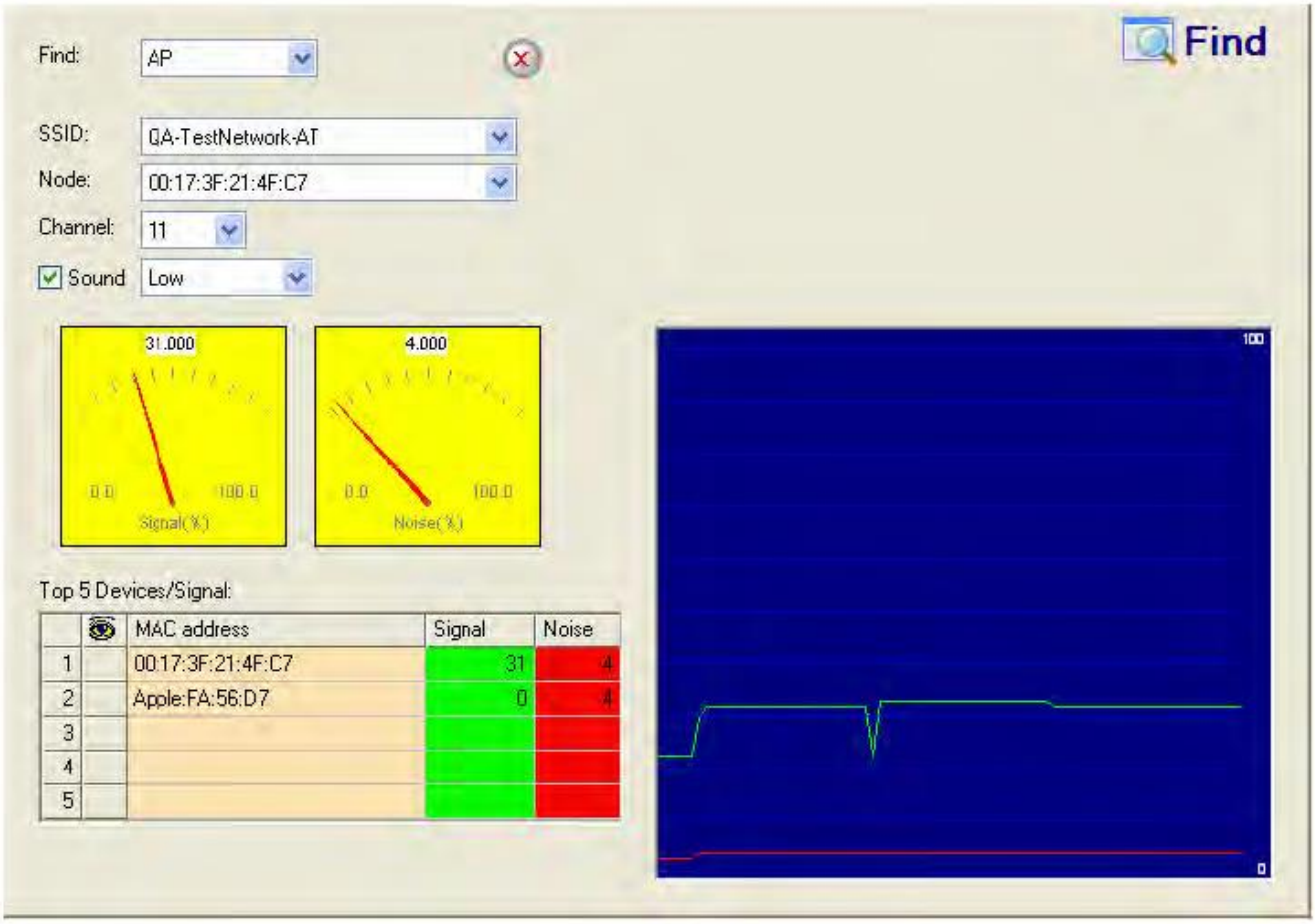
Инструменты спуфинга: SMAC, macchanger, SirMACsAlot, Gentle MAC Pro

Описание сигнала тревоги и возможные причины

Злоумышленник, желающий нарушить работу беспроводной сети, имеет широкий выбор инструментов атаки. Большинство этих инструментов (которые доступны для бесплатной загрузки в Интернете) полагаются на поддельный MAC-адрес, в результате чего устройство злоумышленника маскируется под авторизованную точку беспроводного доступа или клиента. С помощью этих инструментов злоумышленник может запускать различные DoS-атаки (атаки типа «отказ в обслуживании»), обходить механизмы контроля доступа или ложно рекламировать услуги беспроводным клиентам.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает поддельный MAC-адрес, следуя авторизованному IEEE идентификатору производителя (OUI) и сигнатуре порядкового номера кадра 802.11. Администратор или специалист по безопасности беспроводной сети могут использовать инструмент Find (Найти) приложения AirMagnet WiFi Analyzer для отслеживания устройства-нарушителя, следя за отображаемым на экране уровнем сигнала, как показано ниже.



Инструмент Find (Найти) приложения AirMagnet WiFi Analyzer, используемый для обнаружения устройства-нарушителя

Policy – Higher layer protocol problem (Политика - проблема протокола более высокого уровня)

Проблема протокола более высокого уровня.

Denial-of-Service Attack: Association Table Overflow (Атака типа «отказ в обслуживании»: Переполнение таблицы подключений)

Описание сигнала тревоги и возможные причины

Беспроводные злоумышленники могут исчерпать ресурсы точки доступа, в первую очередь таблицу подключения клиентов, путем эмуляции большого количества беспроводных клиентов с поддельными MAC-адресами. Каждый из этих эмулируемых клиентов будет пытаться установить связь и пройти аутентификацию на целевой точке доступа. Аутентификация 802.11 обычно выполняется, потому что в большинстве сетей используется открытая система аутентификации 802.11, которая, по сути, является процессом нулевой аутентификации. Затем за процессом аутентификации будет следовать соединение с этими эмулированными клиентами. Однако эти эмулированные клиенты не будут выполнять аутентификацию более высокого уровня, такую как 802.1x или VPN, оставляя, таким образом, протокол транзакции незавершенным. На этом этапе атакованная точка доступа поддерживает состояние каждого

эмулированного клиента в таблице подключения клиентов. После того как ресурсы точки доступа и таблица подключения клиентов заполнены эмулированными клиентами и информацией об их состоянии, атакуемая точка доступа больше не сможет обслуживать легитимных клиентов. Так организуется атака «отказ в обслуживании».

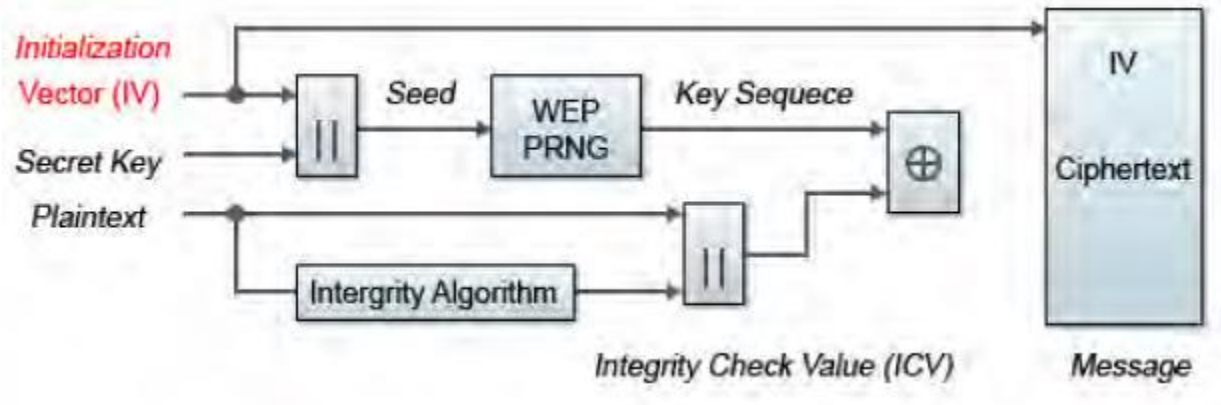
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает процесс аутентификации клиента и определяет признаки DoS-атаки против точки доступа. Незавершенные транзакции аутентификации и подключения запускают процесс обнаружения атак приложением AirMagnet WiFi Analyzer и статистического сопоставления сигнатур.

Crackable WEP IV Key Used (Используется взламываемый ключ WEP IV)

Описание сигнала тревоги и возможные причины

Хорошо известно, что устройство WLAN, использующее для шифрования статический ключ WEP, уязвимо для различных атак взлома ключа WEP (Обратитесь к документу «Weaknesses in the Key Scheduling Algorithm of RC4 – I» (Слабые стороны алгоритма планирования ключей RC4 – I), авторы Scott Fluhrer, Itsik Mantin и Adi Shamir (Скотт Флурер, Ицик Мантин и Ади Шамир)).



Initialization Vector (IV)	Вектор инициализации (IV)
Seed	Сид
Key Sequence	Последовательность ключа
Secret Key	Секретный ключ
Plaintext	Открытый текст
Integrity Algorithm	Алгоритм целостности
Ciphertext	Зашифрованный текст
Integrity Check Value (ICV)	Значение проверки целостности (ICV)
Message	Сообщение

Блок-схема процесса шифрования WEP

Взлом злоумышленником секретного ключа WEP приводит к отсутствию защиты шифрованием, что ставит под угрозу конфиденциальность данных. Ключ WEP, который в большинстве случаев является 64-битным или 128-битным (некоторые производители также предлагают 152-битное шифрование), состоит из секретного ключа, сконфигурированного пользователем, соединенного с 24-битным IV (вектором инициализации). IV определяется передающей станцией. Когда ключ IV повторно используется часто или в последовательных кадрах, это увеличивает вероятность восстановления секретного ключа хакерами, проникающими в беспроводную сеть. Исключая определенные значения IV, которые могут создать так называемые «слабые ключи», можно избежать слабости WEP, описанной в вышеупомянутом документе.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer предупреждает о слабой реализации WEP и для устранения проблемы с использованием IV рекомендует обновить прошивку устройства, запросив ее у

производителя. В идеале корпоративную сеть WLAN можно защитить от уязвимости WEP с помощью шифрования TKIP (Temporal Key Integrity Protocol – Протокол ограниченной по времени целостности ключа), которое поддерживается большинством беспроводного оборудования корпоративного уровня. Устройства с поддержкой TKIP не подвержены атаке по ключу WEP.

Policy – 802.1x authentication failure (Политика - Сбой аутентификации 802.1x)

Ошибка аутентификации 802.1x. Либо пропущены определенные шаги, либо клиент неправильно настроен.

Device Unprotected by VPN (Устройство не защищено VPN)

Описание сигнала тревоги и возможные причины

Если система безопасности вашей сети WLAN требует использования VPN, приложение AirMagnet WiFi Analyzer может предупреждать об устройствах, которые участвуют в беспроводной связи без защиты VPN. Использование защиты VPN в вашей сети WLAN способно помочь обеспечить аутентификацию системы и пользователя, создать динамические ключи для шифрования и обеспечить контроль доступа и (что наиболее важно) качество обслуживания (QoS). Использование VPN в дополнение к WEP в сети также обеспечивает шифрование на всем пути до шлюза VPN. Это может быть очень эффективным для путешествующих сотрудников, использующих сети с публичными точками доступа.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer распознает реализации VPN с использованием IPSec, PPTP, L2TP и SSH в качестве протоколов туннелирования. Сигнал тревоги подается, когда устройства обмениваются данными друг с другом без какой-либо защиты VPN.

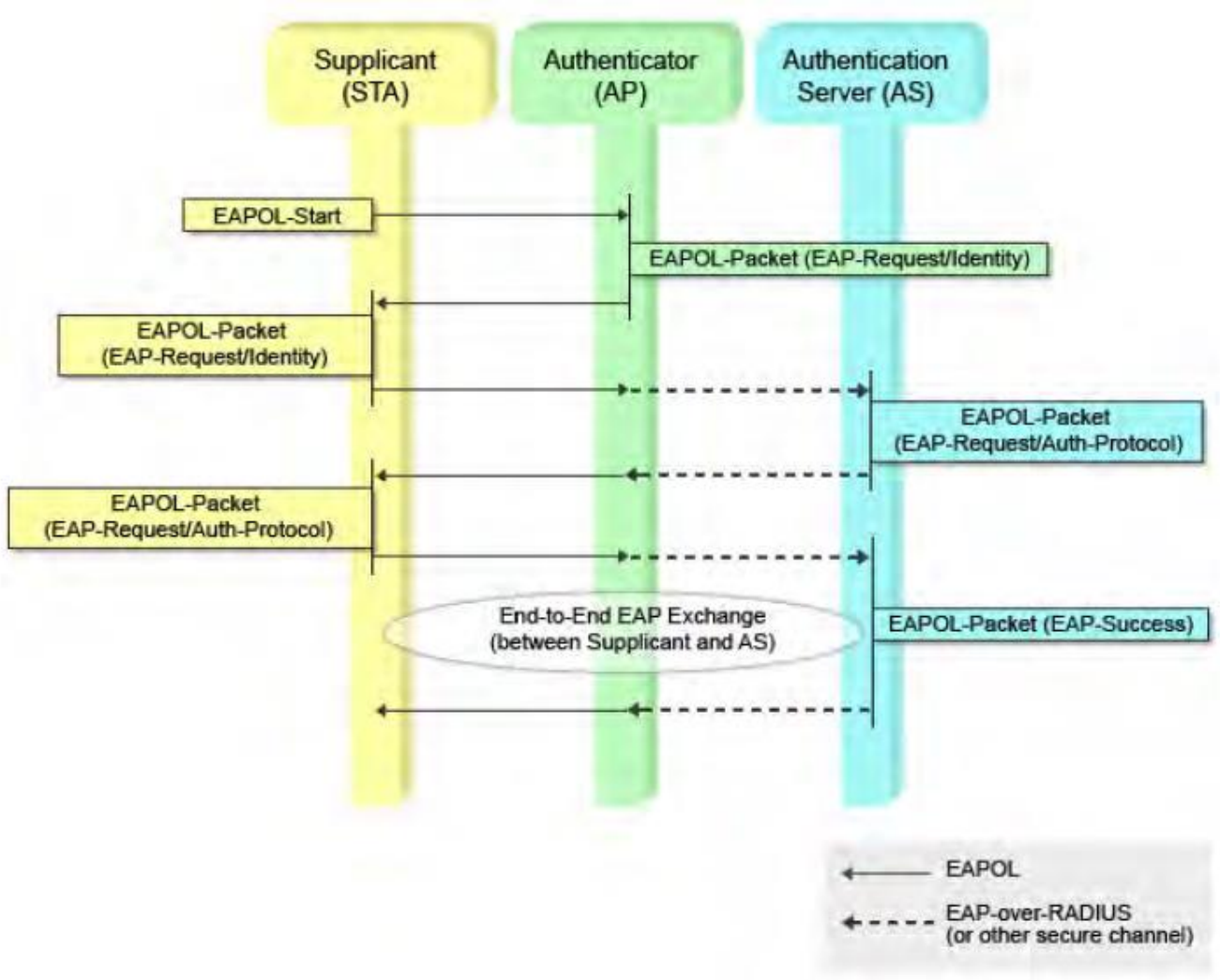
Примечание: Приложение AirMagnet WiFi Analyzer не сможет активировать этот сигнал тревоги, если в вашей беспроводной локальной сети также развернуто такое шифрование 802.11, как 802.1x или TKIP.

Если вы не развертываете VPN как часть инфраструктуры безопасности сети WLAN, эту сигнализацию в приложении AirMagnet WiFi Analyzer можно отключить.

Device Unprotected by 802.1x (Устройство не защищено 802.1x)

Описание сигнала тревоги и возможные причины

Если система безопасности вашей сети WLAN требует для аутентификации и шифрования использования 802.1x, приложение AirMagnet WiFi Analyzer может предупреждать вас об устройствах, которые не настроены для использования защиты 802.1x. WPA (защищенный беспроводной доступ) определяет 802.1x как одно из требований. Инфраструктура 802.1x обеспечивает централизованную аутентификацию пользователей и управление ключами шифрования.



Supplicant (STA)	Проситель (станция)
Authenticator (AP)	Аутентификатор (точка доступа)
Authentication Server (AS)	Сервер аутентификации
EAPoL– Start	EAPoL – Старт
EAPoL-Packet (EAP-Request/Identity)	Пакет EAPoL (EAP-Запрос/Идентификатор)
EAPoL-Packet (EAP-Request/Auth-Protocol)	Пакет EAPoL (EAP-Запрос/Протокол аутентификации)
End-to-End EAP Exchange…	Сквозной обмен EAP (между просителем и сервером аутентификации)
EAPoL-Packet (EAP-Success)	Пакет EAPoL (EAP-Успешно)
EAP-over-RADIUS…	EAP через RADIUS (или другой безопасный канал)

Структура 802.1x обеспечивает централизованную аутентификацию пользователей и управление ключами шифрования

Для реализации механизма аутентификации и шифрования 802.1x используется с различными типами EAP (Extensible Authentication Protocol – Протокол расширенной аутентификации), такими как LEAP, TLS, TTLS, EAP-FAST и PEAP. Если безопасность вашей сети WLAN основана на WPA или 802.1x, не настроенные для 802.1x точки доступа ослабят безопасность WLAN, позволяя несоответствующим пользователям ложно аутентифицироваться и входить в вашу проводную сеть. Неправильно настроенные клиентские станции без защиты 802.1x также представляют угрозу безопасности. Например, у них не будет механизма взаимной аутентификации, обеспечиваемого структурой 802.1x, и поэтому они будут уязвимы для случайного подключения к поддельной точке доступа злоумышленника.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer распознает все типы EAP 802.1x, включая PEAP, TLS, TTLS, LEAP, EAP-FAST и т.д. Путем наблюдения за отклоненными попытками аутентификации 802.1x приложение AirMagnet WiFi Analyzer обнаруживает точки доступа и клиентские станции, не защищенные 802.1x.

Ad-hoc Node Using AP's SSID (Узел Ad-hoc, использующий SSID точки доступа)

Описание сигнала тревоги и возможные причины

Стандарт IEEE 802.11 определяет два режима работы сети WLAN:

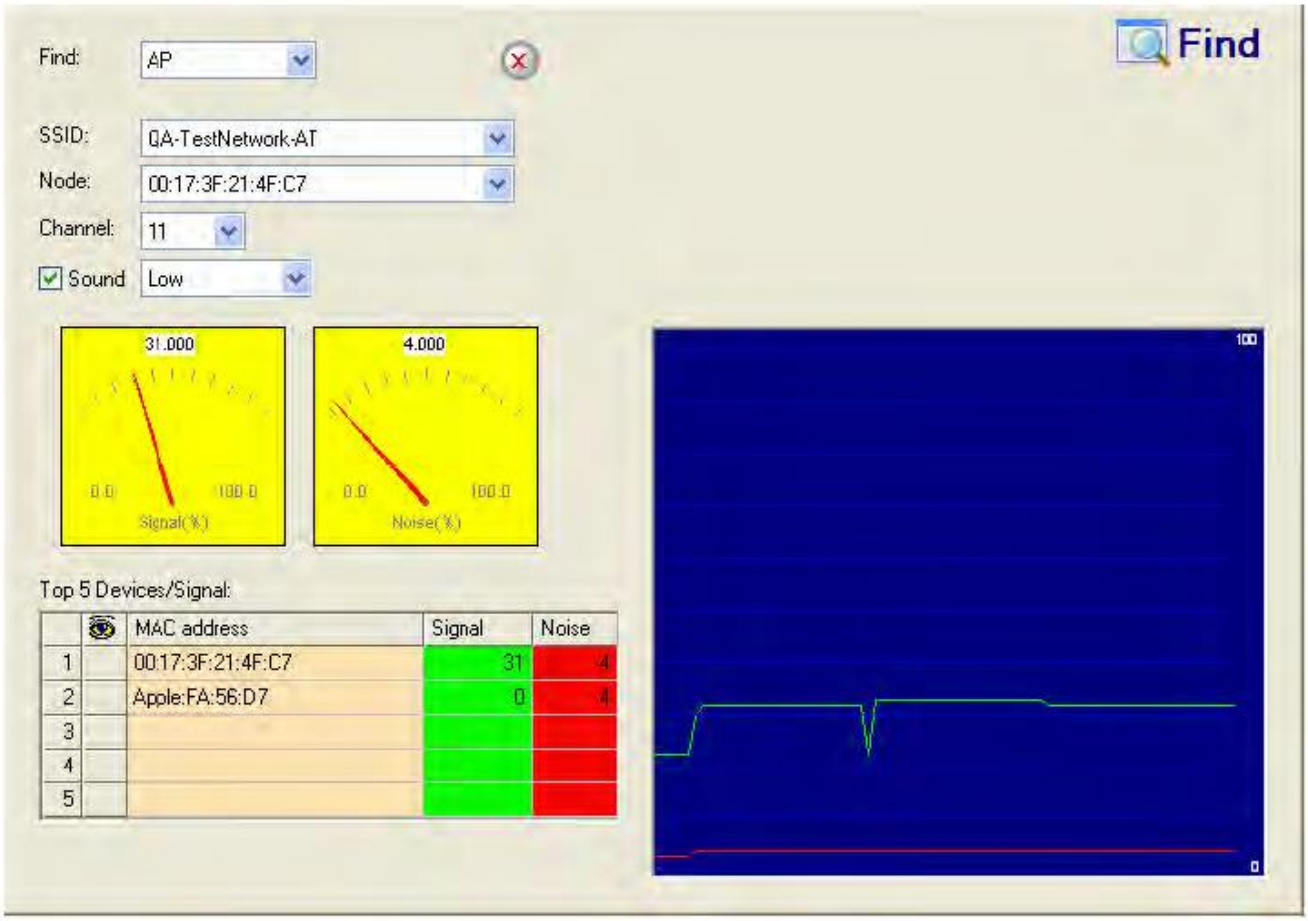
- Режим инфраструктуры (Infrastructure) для сети точек доступа и клиентских станций, а также
- Режим Ad-hoc для одноранговых сетевых соединений между беспроводными клиентами.

Оба режима могут иметь свои собственные идентификаторы SSID и способны сосуществовать в одной радиочастотной среде. Однако когда устройства в режиме инфраструктуры и в режиме ad-hoc используют один и тот же идентификатор SSID, клиентские соединения могут стать ненадежными и несовместимыми. Для сетей WLAN в режиме инфраструктуры и в режиме ad-hoc должны использоваться отдельные идентификаторы SSID.

Зачастую использование одного идентификатора SSID устройствами в режиме инфраструктуры и в режиме ad-hoc вызвано неправильной настройкой конфигурации. Такая неправильная конфигурация может вызвать проблемы с подключением не только для неправильно настроенного устройства, но и для всех клиентов в этой области.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает совместное использование идентификатора SSID устройствами в режиме инфраструктуры и устройствами в режиме ad-hoc и подает сигнал тревоги для раннего предупреждения. Найдите устройство ad-hoc и заставьте пользователя использовать другой идентификатор SSID для одноранговой соединения с другими устройствами ad-hoc. После идентификации устройства ad-hoc и получения сообщения от приложения AirMagnet WiFi Analyzer администратор сети WLAN может для его поиска использовать инструмент FIND (Найти).

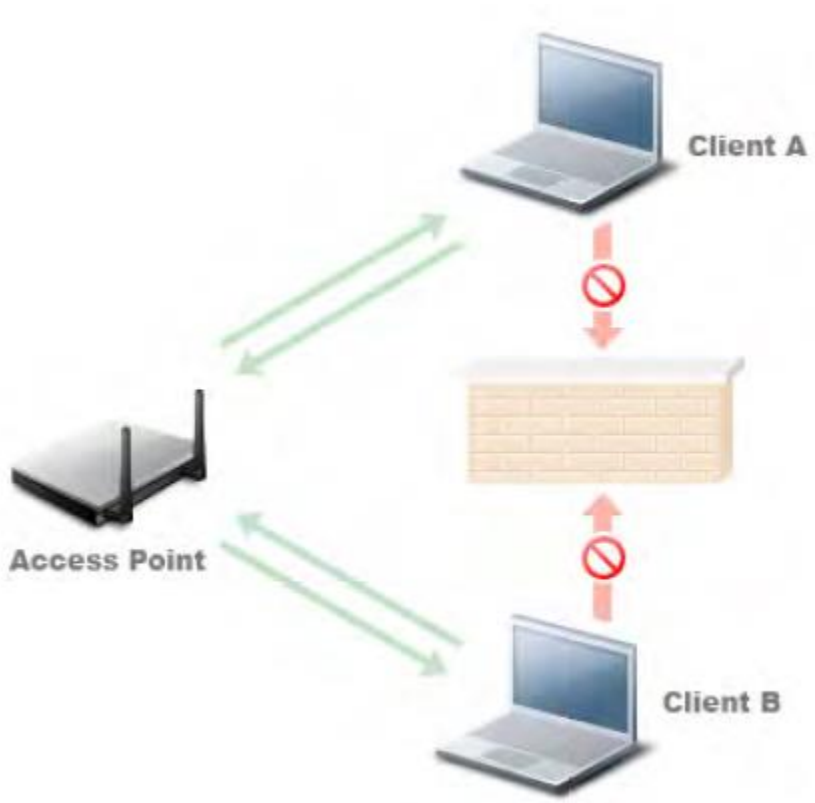


Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Hidden Station Detected (Обнаружена скрытая станция)

Описание сигнала тревоги и возможные причины

Проблема со скрытой станцией возникает, когда беспроводной узел не может услышать один или несколько других узлов, и, следовательно, протокол доступа к среде (CSMA/CA - Многостанционный доступ с контролем несущей и недопущением конфликтов) не способен работать должным образом. В этом случае несколько узлов будут одновременно пытаться передать свои данные по совместно используемой среде, вызывая взаимные помехи. Представьте, например, что есть два конечных пользователя 802.11 (станция A и станция B) и одна точка доступа. Станция A и станция B не слышат друг друга из-за сильного затухания (например, большого расстояния между ними), но обе могут подключиться к одной и той же точке доступа. Из-за этой ситуации станция A может начать передачу кадра, не замечая, что станция B в настоящее время тоже осуществляет передачу (или наоборот). Это может вызвать конфликт между станцией A и станцией B в точке доступа. В результате и станции A, и станции B потребуется повторно передать соответствующие пакеты, что приведет к увеличению служебных данных и снижению пропускной способности сети.



Client A (B)	Клиент A (B)
Access Point	Точка доступа

Проблема со скрытым узлом – коллизия трафика от станции A и станции B в точке доступа

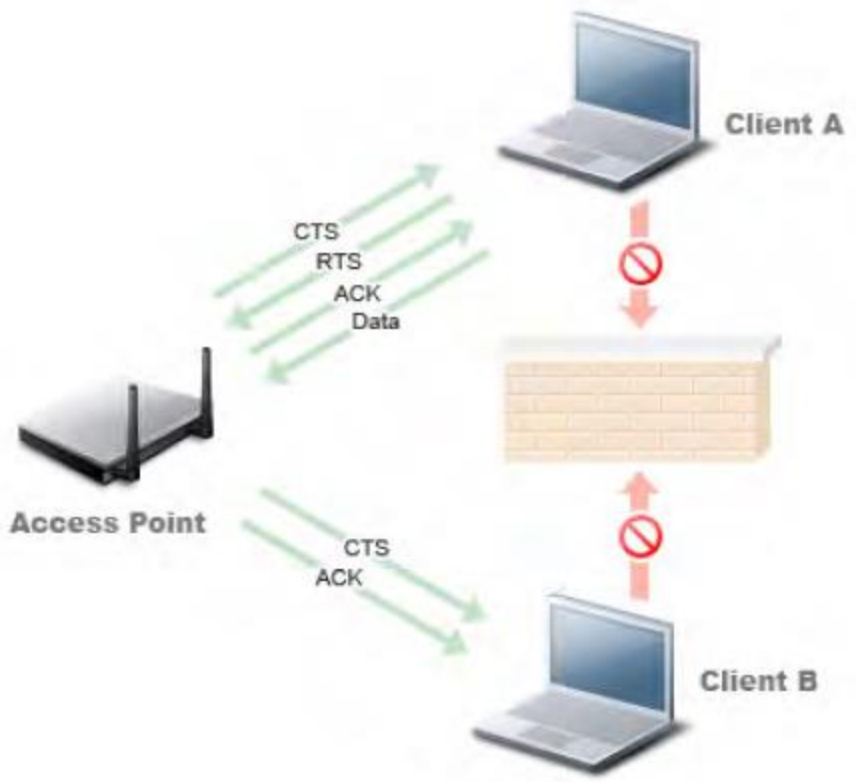
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает проблему со скрытым узлом, определяя местоположение скрытой станции. Например, если установить анализатор Wi-Fi AirMagnet в указанном выше месте станции A, он будет пассивно прослушивать и анализировать трафик, полученный в этом месте, и определять все станции, скрытые от этого местоположения (местоположения, где находится сам анализатор AirMagnet). После обнаружения скрытых станций приложение AirMagnet WiFi Analyzer предложит меры противодействия, обычно включение механизма RTS/CTS (готовность к передаче/готовность к приему) для координации доступа к среде передачи. В приведенном выше примере можно было бы перенастроить станцию A и станцию B таким образом, чтобы иметь очень низкий порог (размер пакета) для запуска использования RTS и CTS.

Source	Источник
RTS	Готовность к передаче
CTS	Готовность к приему

Data	Данные
ACK	Подтверждение
Destination	Адресат (место назначения)

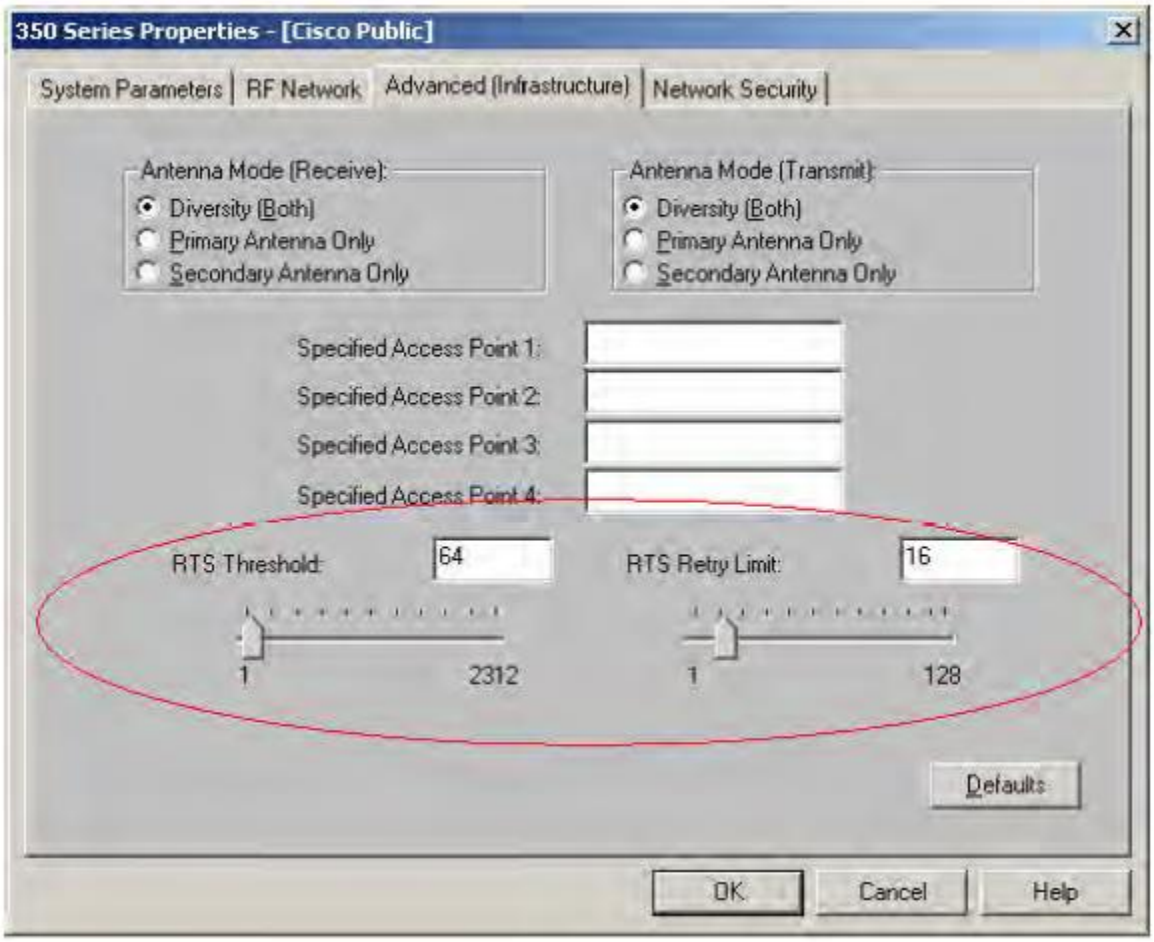
Механизм RTS/CTS, предназначенный для синхронизации доступа к беспроводной среде перед передачей данных



Client A (B)	Клиент A (B)
CTS	Готовность к приему
RTS	Готовность к передаче
ACK	Подтверждение
Data	Данные
Access Point	Точка доступа

Механизм RTS/CTS решает проблему со скрытым узлом

Чтобы настроить устройство для использования RTS/CTS, пожалуйста, обратитесь к приведенному ниже примеру настройки конфигурации Cisco:



Пример настройки конфигурации RTS/CTS для клиентского адаптера Cisco Aironet, позволяющий устранить проблему со скрытым узлом

Unassociated Station Detected (Обнаружена неподключенная станция)

Описание сигнала тревоги и возможные причины

Если беспроводная клиентская станция не смогла пройти аутентификацию или установить связь с точкой доступа, она будет периодически продолжать такие попытки, пока не будет установлено успешное соединение для осуществления нормальной связи. Приложение AirMagnet WiFi Analyzer обнаруживает клиентские станции, застрявшие в режиме постоянной повторной передачи, чтобы предупредить администратора WLAN о двух вещах:

- Пользователь отключен от беспроводной сети и нуждается в помощи.
- Если приложение AirMagnet Wi-Fi Analyzer сообщает, что несколько пользователей находятся в неподключенном режиме, то может не работать беспроводная инфраструктура (точка доступа или внутренний сервер аутентификации).

Решение AirMagnet

Приложение AirMagnet Wi-Fi Analyzer передает этот сигнал тревоги вместе с идентификатором SSID неподключенной клиентской станции. Для проактивного обнаружения проблем с подключением или аутентификацией для определенной неподключенной станции администратор WLAN может использовать инструмент диагностики (AirMagnet Diagnostic Tool).
В качестве альтернативы администратор WLAN может также использовать инструменты активного сквозного тестирования приложения AirMagnet WiFi Analyzer для дальнейшего исследования проблемы путем эмуляции клиентской станции в операции подключения, DHCP, Ping и Trace route.

AP System or Firmware Reset (Сброс системы или прошивки точки доступа)

Описание сигнала тревоги и возможные причины

Точка беспроводного доступа выполняет сброс системы или прошивки в случае перенастройки, сбоя питания или неисправности программного обеспечения. Когда происходит системный сброс, все ранее подключенные клиентские станции теряют свои соединения до тех пор, пока точка доступа не завершит выполнение последовательности действий при запуске. Для восстановления беспроводного соединения все клиентские станции должны пройти процедуру аутентификации и подключения. Период потери связи может составлять от десятков секунд до нескольких минут.
Поскольку сброс точки доступа является временным, и беспроводное обслуживание в конечном итоге восстанавливается, обычно остается очень мало следов, позволяющих связать его с потерянным подключением клиента.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer может точно обнаруживать системный сброс точки доступа независимо от его причины. С помощью этого сигнала тревоги приложение AirMagnet WiFi Analyzer в подобной ситуации способно установить связь между прерыванием обслуживания и его основной причиной.

AP Broadcasting SSID (Точка доступа с вещанием SSID)

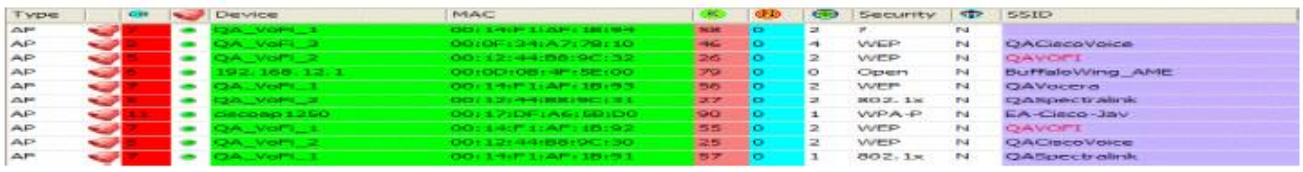
Описание сигнала тревоги и возможные причины

Идентификаторы SSID в сети WLAN обычно объявляются в кадрах маяка, передаваемых точками доступа. Они предназначены для того, чтобы клиентские станции легко идентифицировали доступные сети WLAN и точки доступа, предоставляющие беспроводные услуги. Передвигающиеся на автомобилях злоумышленники, оснащенные такими инструментами, как Netstumbler, иногда сканируют отправляемые точками доступа идентификаторы SSID для обнаружения потенциальных целей. Если идентификатор SSID сети WLAN открыт, ваша сеть может быть подвержена двум конкретным угрозам:

- Злоумышленники могут установить SSID на своем клиенте, чтобы попытаться подсоединиться к этой сети WLAN. Согласно большинству веб-сайтов вардрайверов, многие используемые в наши дни точки доступа работают без какого-либо обеспечения безопасности. Несмотря на то, что знание имени SSID не обязательно означает, что мошеннические клиенты смогут подключиться к сети, необходимо беспокоиться и о других формах атак на безопасность (например, DoS-атаках).
- Информация о географическом местоположении сети WLAN и точек доступа с координатами GPS может собираться в глобальной базе данных и публиковаться в Интернете.

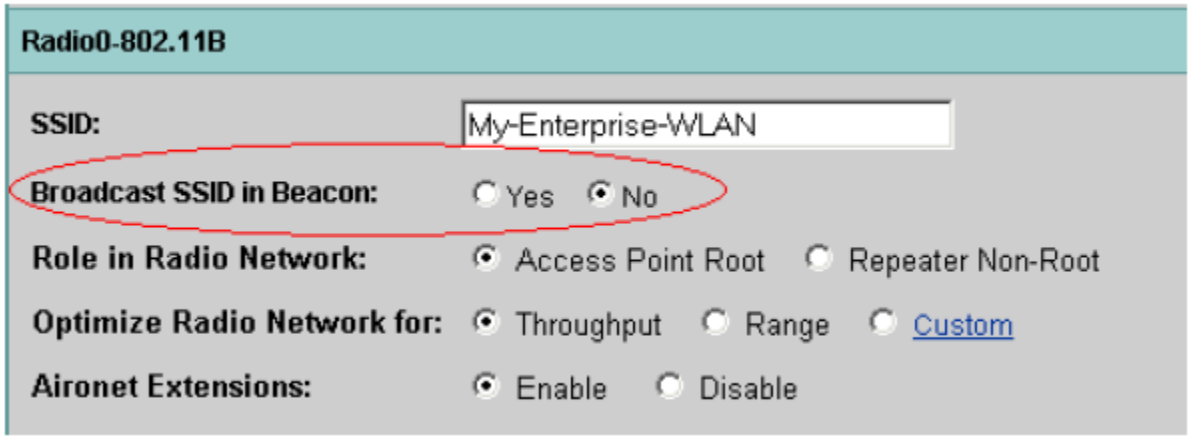
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает точку доступа, транслирующую свой идентификатор SSID, и запускает сигналы тревоги (также приложение может обнаруживать SSID, которые не транслируются). На странице Start приложения идентификатор SSID точки доступа обозначен красным цветом, если этот SSID не является широковещательным. Смотрите приведенные ниже скриншоты экранов AirMagnet:



На странице START красным цветом отображается нешироковещательный SSID.

Большинство производителей точек доступа поддерживают широковещательную конфигурацию идентификатора SSID. Точку доступа Cisco Aironet можно настроить из Интернет-браузера (смотрите рисунок ниже).



Отключение трансляции идентификатора SSID для точки доступа Cisco Aironet через интерфейс браузера

Ad-hoc Station Detected (Обнаружена станция Ad-hoc)

Описание сигнала тревоги и возможные причины

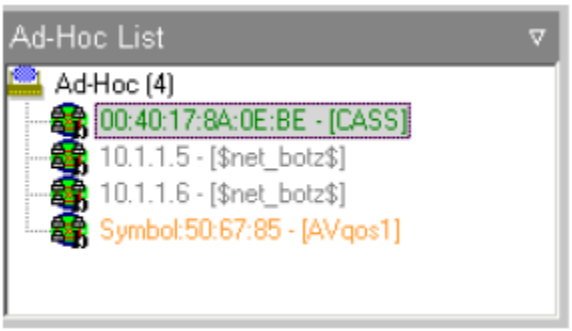
Беспроводная клиентская станция, работающая в режиме ad-hoc (одноранговая сеть), обычно не защищена теми же строгими правилами безопасности, что и точки доступа, разворачиваемые на корпоративной сети в режиме инфраструктуры.

Сетевое соединение в режиме Ad-hoc (одноранговая станция) в обход инфраструктуры безопасности предприятия

Обычно корпоративные сети WLAN не поддерживают одноранговые сети и, следовательно, не имеют необходимых мер безопасности, таких как аутентификация пользователя 802.1x и шифрование с динамическим ключом. В результате станции, работающие в режиме ad-hoc, рискуют раскрыть передаваемые в эфире данные из-за слабого шифрования (если таковое имеется). Кроме того, слабая аутентификация даст возможность подключения неавторизованным устройствам. Если клиентская станция в режиме ad-hoc также подключена к проводной сети, под угрозой находится вся проводная сеть предприятия. Из-за высокого риска клиентскую станцию в режиме Ad-hoc следует исследовать как неавторизованную точку доступа.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает использование режима ad-hoc и подает сигналы тревоги. Для получения списка всех станций в режиме ad-hoc можно использовать экран Infrastructure (Инфраструктура). Смотрите рисунок ниже:



Для проверки безопасности все станции в режиме Ad-hoc идентифицированы на странице Infrastructure (Инфраструктура)

После срабатывания этого сигнала тревоги устройство ad-hoc можно найти с помощью инструмента Find (Найти), и затем удалить его из корпоративной сети.

High Management Traffic Overhead (Высокие служебные данные трафика менеджмента)

Описание сигнала тревоги и возможные причины

Стандарт IEEE 802.11 определяет три основных типа кадров: кадры менеджмента, кадры управления и кадры данных. Кадры менеджмента (такие как кадры маяка, зондирующий запрос/ответ, запрос/ответ соединения, аутентификация и т.д.) не несут пользовательские данные, но необходимы для облегчения установки соединения. Они считаются необходимыми для работы WLAN служебными данными.

Тип кадра (биты 2, 3)	Субполе (биты 7, 6, 5, 4)	Функция кадра
Менеджмент 00	0000 0001 0010 0011 0100 0101 1000 1001 1010 1011 1100	Запрос подключения Ответ на запрос подключения Запрос подключения Ответ на запрос повторного подключения Ответ на зондирующий запрос Ответ на зондирующий запрос Сигнал маяка ATIM (Индикация объявляемого трафика) Отключение Аутентификация Деаутентификация
Управление 01	1010 1011 1100 1110 1111	Запрос энергосбережения (PS) Готовность к передаче (RTS) Подтверждение (ACK) Завершение периода, свободного от конкуренции (CF) Завершение CF + подтверждение CF
Данные 10	0000 0001 0010 0011 0100 0101 1010 1011	Данные Данные + CF ACK Данные + CF Poll Данные + CF ACK + CF Poll Нуль (нет данных) CF ACK CF Poll CF ACK + CF Poll
Зарезервировано 11		

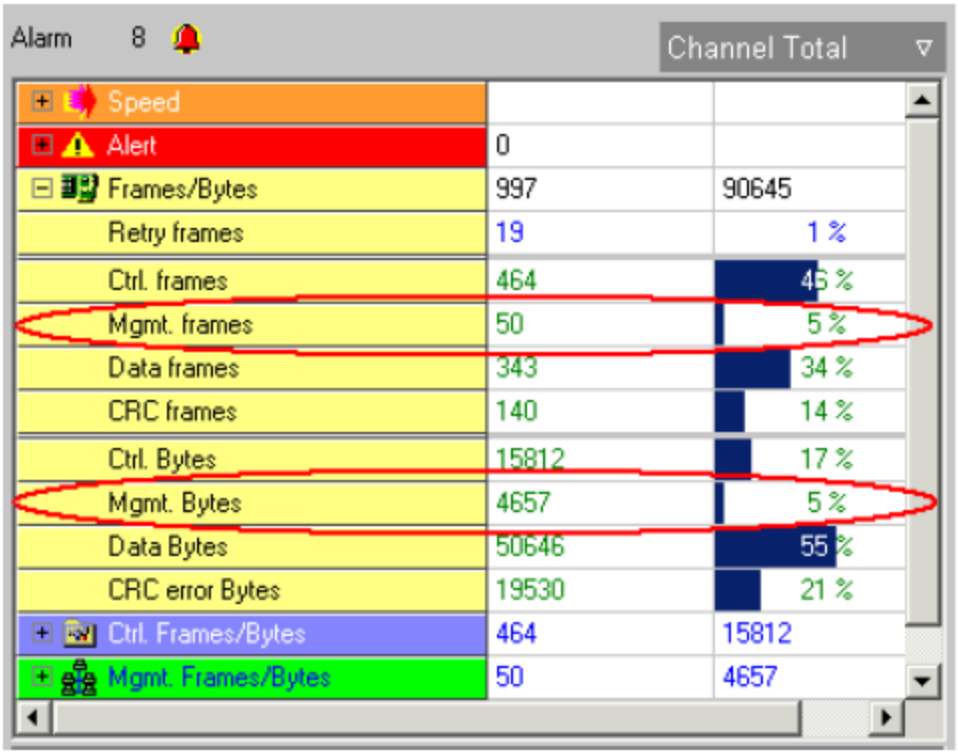
Типы кадров 802.11 для менеджмента, управления и передачи данных

Кадры менеджмента передаются с низкой скоростью (1 Мбит/с или 2 Мбит/с для 802.11b) и, следовательно, потребляют больше полосы пропускания WLAN, чем кадры данных. В эффективной сети WLAN использование полосы пропускания канала трафиком кадров менеджмента должно быть довольно

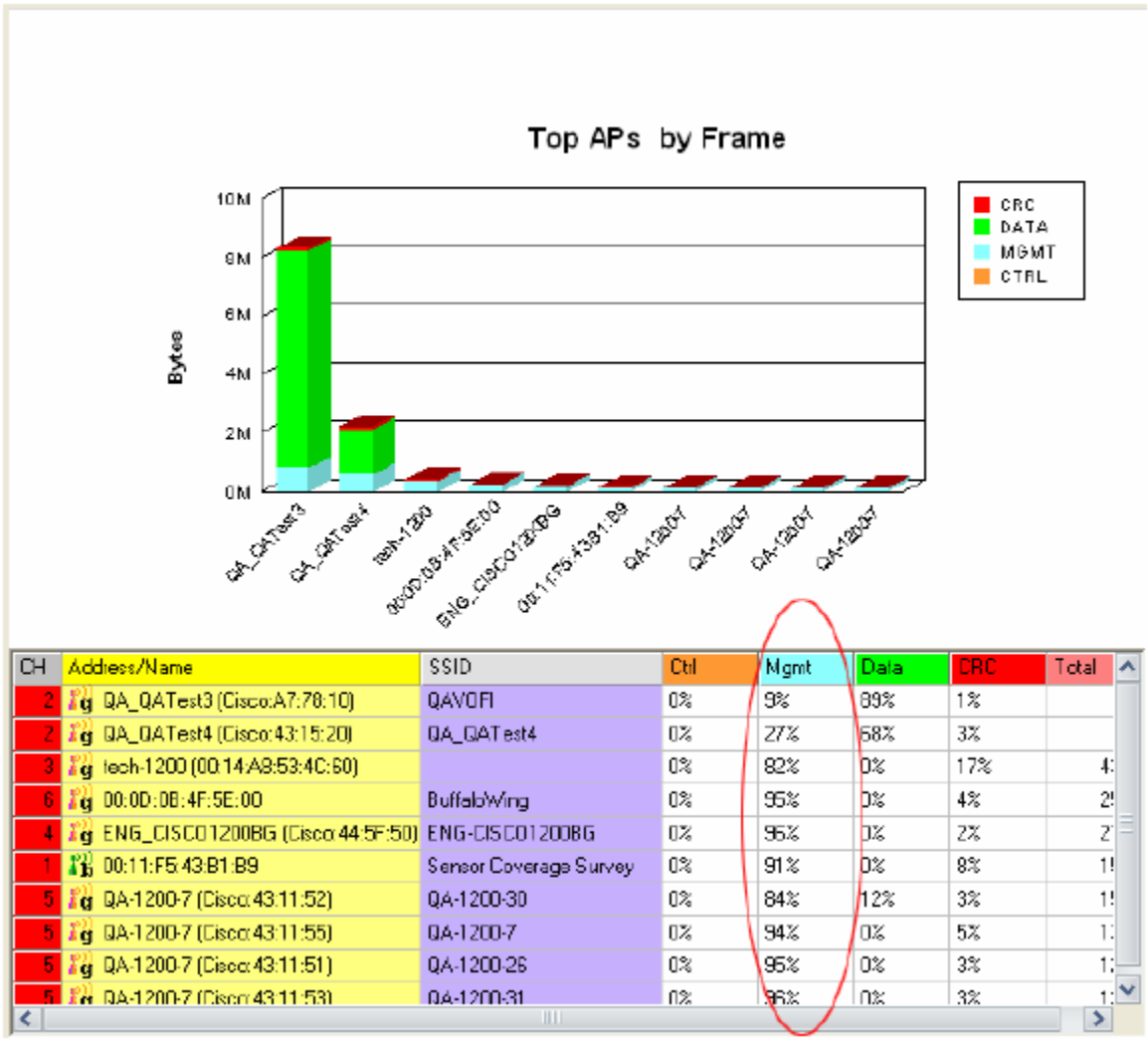
низким (менее 1%). Высокий процент трафика кадров менеджмента сам по себе является проблемой с точки зрения потребления полосы пропускания, и также может указывать на более серьезные проблемы. Например, если большое количество клиентских станций не могут подключиться к точке доступа, они постоянно совершают повторные попытки подключения, что приводит к большому объему трафика менеджмента.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает трафик менеджмента и соответствующее использование полосы пропускания для каждого канала и устройства. При превышении установленного пользователем порога использования срабатывают сигналы тревоги. Чтобы определить причину проблемы с большим объемом служебных данных на управление, администратор WLAN может исследовать ее с помощью экрана Channel (Канал) или Charts (Графики). Примеры снимков экрана приводятся ниже:



На странице Channel (Канал) отображается статистика для кадров менеджмента.



CH	Address/Name	SSID	Ctl	Mgmt	Data	CRC	Total
2	QA_QATest3 (Cisco:A7:78:10)	QAVOFI	0%	9%	89%	1%	
2	QA_QATest4 (Cisco:43:15:20)	QA_QATest4	0%	27%	68%	3%	
3	tech-1200 (00:14:A8:53:4C:60)		0%	82%	0%	17%	4
6	00:0D:0B:4F:5E:00	BuffaloWing	0%	95%	0%	4%	2
4	ENG_CISCO1200BG (Cisco:44:5F:50)	ENG-CISCO1200BG	0%	96%	0%	2%	2
1	00:11:F5:43:B1:B9	Sensor Coverage Survey	0%	91%	0%	8%	1
5	QA-1200-7 (Cisco:43:11:52)	QA-1200-30	0%	84%	12%	3%	1
5	QA-1200-7 (Cisco:43:11:55)	QA-1200-7	0%	94%	0%	5%	1
5	QA-1200-7 (Cisco:43:11:51)	QA-1200-26	0%	95%	0%	3%	1
5	QA-1200-7 (Cisco:43:11:53)	QA-1200-31	0%	96%	0%	3%	1

На странице Channel (Канал) отображается распределение трафика между кадрами менеджмента/данных/управления по каналам или по устройствам.

AP Overloaded by Stations (Точка доступа перегружена станциями)

Описание сигнала тревоги и возможные причины

Точка доступа WLAN имеет ограниченные ресурсы и поэтому может обслуживать только ограниченное количество клиентов. При достижении предела дополнительные клиенты могут обнаружить, что их запросы на обслуживание отклонены, или у существующих клиентов может снизиться производительность. Данное ограничение следует учитывать при проектировании развертывания оборудования и предоставлении услуг WLAN. По мере роста числа пользователей после развертывания сети существующему оборудованию может стать все труднее поддерживать постоянное обслуживание. Эта ситуация требует непрерывного контроля на случай возникновения проблем.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает рабочую нагрузку точки доступа, контролируя ее активные клиентские станции. Систему можно настроить на подачу сигналов тревоги разного уровня серьезности по порогу рабочей нагрузки (количество активных клиентских сеансов), например, предупреждения для 64 активных клиентских сеансов и срочный сигнал тревоги для 128 активных клиентских сеансов. Для исследования текущих клиентских сеансов точки доступа можно использовать экран Infrastructure (Инфраструктура). Если часто возникает перегрузка нескольких точек доступа, рекомендуется либо уменьшить количество подключающихся к сети клиентов, либо увеличить количество установленных точек доступа.

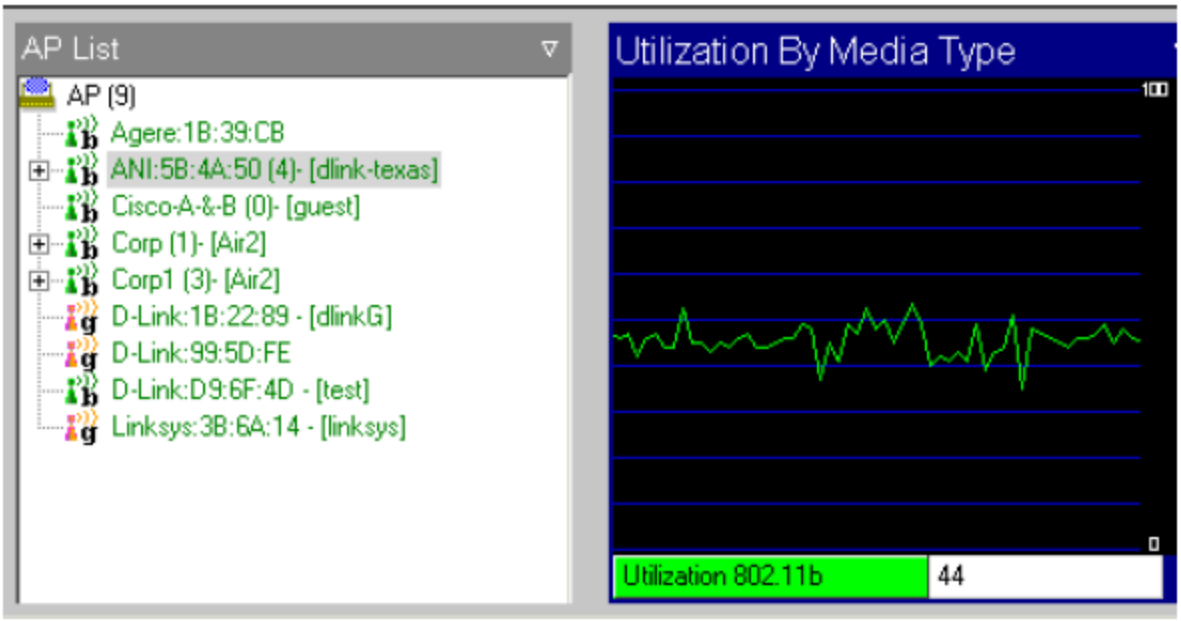
AP Overloaded by Utilization (Точка доступа перегружена по использованию)

Описание сигнала тревоги и возможные причины

Конструкция развертываемой сети WLAN обычно предполагает наличие максимального количества клиентов, которое может поддерживать точка доступа. Точно так же ожидается максимальное использование полосы пропускания, поддерживаемой точкой доступа. Подобные ожидания можно использовать для отслеживания достаточной подготовки сети WLAN и эффективной балансировки нагрузки в ней.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает использование полосы пропускания точки доступа (сумму исходящего и входящего трафика) и подает сигнал тревоги, когда устойчивое использование превышает установленное пользователем пороговое значение. Для дальнейшего изучения использования полосы пропускания точки доступа можно использовать экран Infrastructure (Инфраструктура), который позволяет определить станции, связанные с этой точкой доступа, и их индивидуального потребления полосы пропускания при передаче от точки доступа и к ней. Также для определения наиболее активных участников беспроводной сети и соответствующее распределение их трафика по типу/скорости можно использовать экран Charts (Диаграммы). Если часто возникает перегрузка определенных точек доступа, рекомендуется либо уменьшить количество подключающихся к сети клиентов, либо увеличить количество установленных точек доступа.



На странице инфраструктуры (Infrastructure) отображается использование полосы пропускания точки доступа

802.1x Rekey Timeout Too Long (Слишком долгий таймаут смены ключа 802.1x)

Описание сигнала тревоги и возможные причины

Широко известно, что устройства WLAN, использующие для шифрования статический ключ WEP, уязвимы для атаки взлома ключа WEP (Обратитесь к документу «Weaknesses in the Key Scheduling Algorithm of RC4 – I» (Слабые стороны алгоритма планирования ключей RC4 – I), авторы Scott Fluhrer, Itsik Mantin и Adi Shamir (Скотт Флурер, Ицик Мантин и Ади Шамир)). Взлом секретного ключа WEP приводит к отсутствию защиты с помощью шифрования, что ставит под угрозу конфиденциальность данных в сети. Такие механизмы динамического шифрования или ротации ключей, как TKIP, устраняют подобные уязвимости, периодически меняя ключ шифрования даже в рамках одного сеанса. Управление ротацией ключей для

многоадресного и широковещательного трафика обычно является более сложной задачей, поскольку несколько устройств должны синхронно обновлять ключ. Реализация производителями ротации ключей при многоадресной/широковещательной рассылке может изменяться от нулевой до полной. Когда ключ многоадресной и широковещательной рассылки не меняется или меняется редко, он так же слаб, как статический WEP, который является объектом атак восстановления ключа.

Постоянно отслеживая транзакции аутентификации и шифрования WLAN 802.1x, приложение AirMagnet Wi-Fi Analyzer способно обнаружить точку доступа, настроенную без ротации ключей шифрования или имеющую продолжительный таймаут ротации ключей. Для конфигураций WLAN 802.1x важно включать разумный таймаут смены ключа шифрования, поскольку устаревший ключ шифрования делает ваше шифрование статическим и таким же уязвимым, как шифрование с использованием статического ключа WEP. Механизм смены ключей должен применяться к одноадресным, многоадресным и широковещательным потокам данных. Устройства с поддержкой TKIP (Temporal Key Integrity Protocol - Протокол ограничения по времени целостности ключа) реализуют алгоритм хеширования (расстановки) ключей WEP и обычно меняют ключи в своих одноадресных потоках данных, но не всегда в многоадресных или широковещательных потоках данных.

Решение AirMagnet

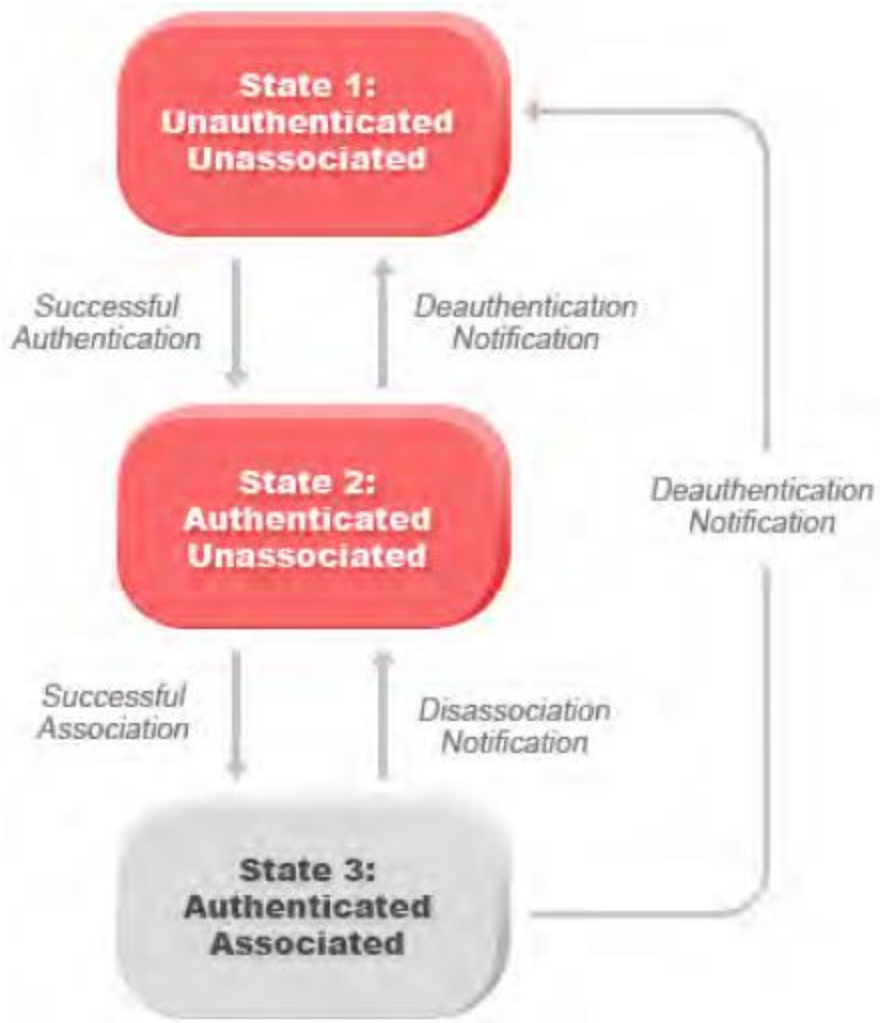
Этот сигнал тревоги приложения AirMagnet WiFi Analyzer помогает задействовать механизм смены ключей для всех потоков данных. Примите соответствующие меры (например, проверьте настройку этого параметра в конфигурации точки доступа), чтобы решить эту проблему.

Denial-of-Service Attack: Authentication Flood (Атака типа «отказ в обслуживании»: Флуд аутентификации)

Инструмент потенциальной атаки: Void11

Описание сигнала тревоги и возможные причины

Для отслеживания аутентификации станции и проверки статуса ее подключения IEEE 802.11 задает машину состояний клиента. Беспроводные клиенты и точки доступа реализуют такую машину состояний (смотрите рисунок ниже) на основе стандарта IEEE. На точке доступа каждая клиентская станция имеет состояние, записанное в таблице клиентов точки доступа (таблице подключений), которая всегда имеет ограничение по размеру, которое может быть либо жестко закодированным числом, либо основанным на ограничении физической памяти.



State 1: …	Состояние 1: Аутентификация не пройдена, нет соединения
Successful Authentication	Успешная аутентификация
Deauthentication Notification	Извещение о деаутентификации
State 2:…	Состояние 2: Аутентификация пройдена, нет соединения
Successful Association	Успешное подключение
Diassociation Notification	Извещение о разъединении
State 3:…	Состояние 3: Аутентификация пройдена, соединение установлено

Злоумышленник подделывает множество запросов аутентификации 802.11, чтобы заполнить таблицу подключения точки доступа клиентами, застрявшими в состоянии 1 и состоянии 2

Форма атаки типа «отказ в обслуживании» направлена на заполнение таблицы состояний клиентов на точке доступа (таблица подключения) путем имитации множества клиентских станций (подмена MAC-адреса), отправляющих на точку доступа запросы аутентификации. После приема каждого индивидуального запроса аутентификации целевая точка доступа должна создать в таблице подключений запись клиента в состоянии 1. Если на точке доступа используется аутентификация Open System, она отправит обратно кадр успешной аутентификации и переведет клиента в состояние 2. Если же на точке доступа используется аутентификация с совместно используемым ключом, точка доступа отправит запрос аутентификации эмулированному злоумышленником клиенту, который не ответит. В этом случае точка доступа сохранит для клиента состояние 1. В любом случае точка доступа закончит на том, что многие клиенты будут находиться либо в состоянии 1, либо в состоянии 2, заполняя таблицу подключения на точке доступа. Когда таблица достигает своего предела, легитимные клиенты не смогут пройти аутентификацию и подключиться к этой точке доступа, поэтому это будет атака типа «отказ в обслуживании».

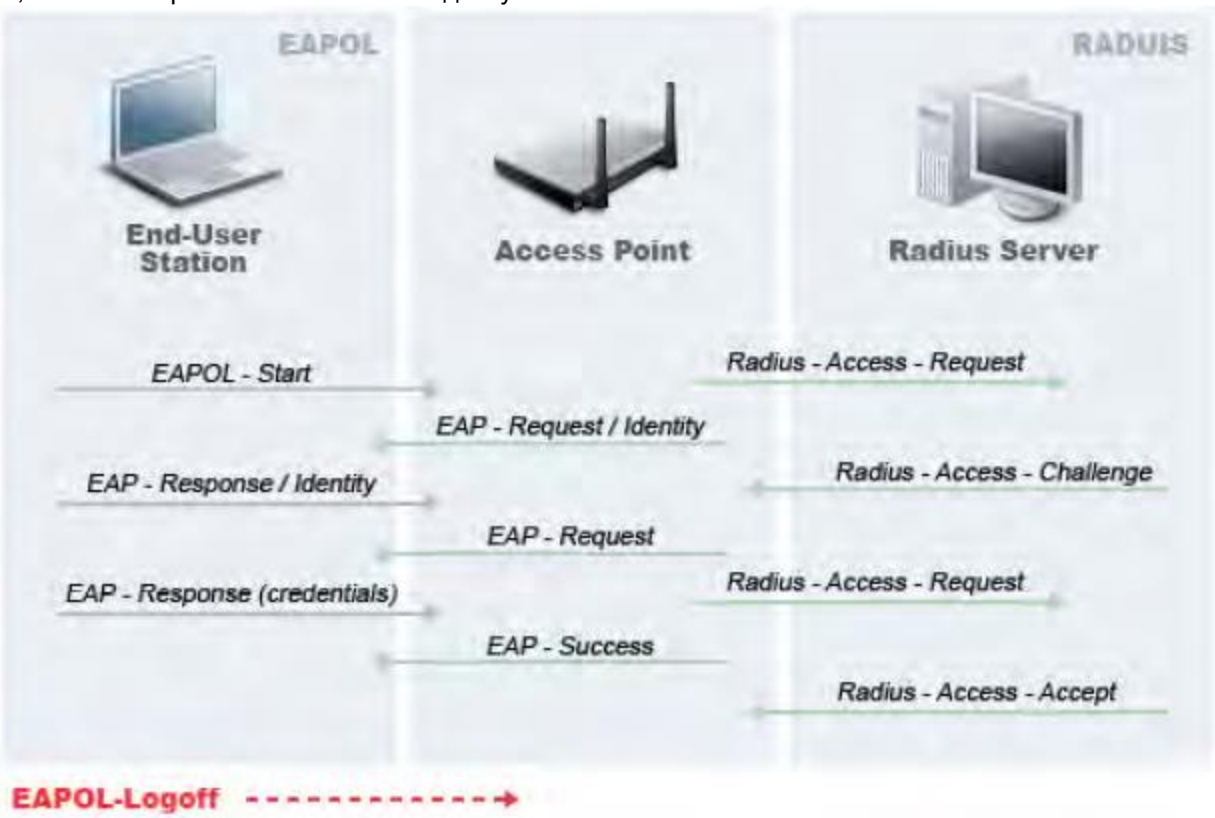
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает эту форму DoS-атаки, отслеживая аутентификацию клиента и состояние подключения. При срабатывании сигнала тревоги будет идентифицирована атакованная точка доступа. Аналитик безопасности WLAN может войти в точку доступа, чтобы проверить текущее состояние таблицы подключений, или использовать активный инструмент AirMagnet (DHCP, ping) для проверки беспроводных услуг, предоставляемых этой точкой доступа.

Denial-of-Service Attack: EAPOL-Logoff Attack (Атака типа «отказ в обслуживании»: Атака EAPOL-Logoff)

Описание сигнала тревоги и возможные причины

Стандарт IEEE 802.1x определяет протокол аутентификации с использованием EAP (Extensible Authentication Protocol – протокол расширенной аутентификации) в локальных сетях или EAPOL. Для начала транзакции аутентификации протокол 802.1x начинается с кадра EAPOL-Start. Когда в конце разрешенного сеанса клиентская станция желает выйти из системы, то отправляет кадр 802.1x EAPOL-Logoff, чтобы завершить сеанс с точкой доступа.



End-User Station	Станция конечного пользователя
Access Point	Точка доступа
Radius Server	Сервер Radius
EAPOL– Start	EAPOL – Старт
Radius –Access – Request	Radius – Доступ – Запрос
EAP-Request/Identity	EAP-Запрос/Идентификатор
EAP-Response/Identity	EAP-Ответ/Идентификатор
Radius –Access – Challenge	Radius – Доступ – Требование
EAP-Request	EAP-Запрос
EAP-Response (credentials)	EAP-Ответ (учетные данные)
Radius –Access – Request	Radius – Доступ – Запрос
EAP-Success	EAP-Успешно
Radius –Access – Accept	Radius – Доступ – Принято
EAPOL-Logoff	EAPOL-Выход

Злоумышленник подделывает кадр 802.1x EAPOL-Logoff с легитимной клиентской станции, чтобы обмануть точку доступа о выходе клиента из системы

Поскольку кадр EAPOL-Logoff не аутентифицирован, злоумышленник может потенциально его подделать, отключив пользователя от точки доступа и совершив таким образом атаку типа «отказ в обслуживании». В то время как эта клиентская станция отключена от точки доступа с использованием подделанного злоумышленником кадра EAPOL-Logoff, клиентская станция фактически не знает об этом до тех пор, пока не попытается снова использовать сеть WLAN. Как правило, обнаружив состояние прерванного соединения, клиентская станция автоматически повторно устанавливает соединение и аутентифицируется, чтобы восстановить подключение к беспроводной сети. Злоумышленник может непрерывно передавать поддельные кадры EAPOL-Logoff, эффективно продолжая эту атаку.

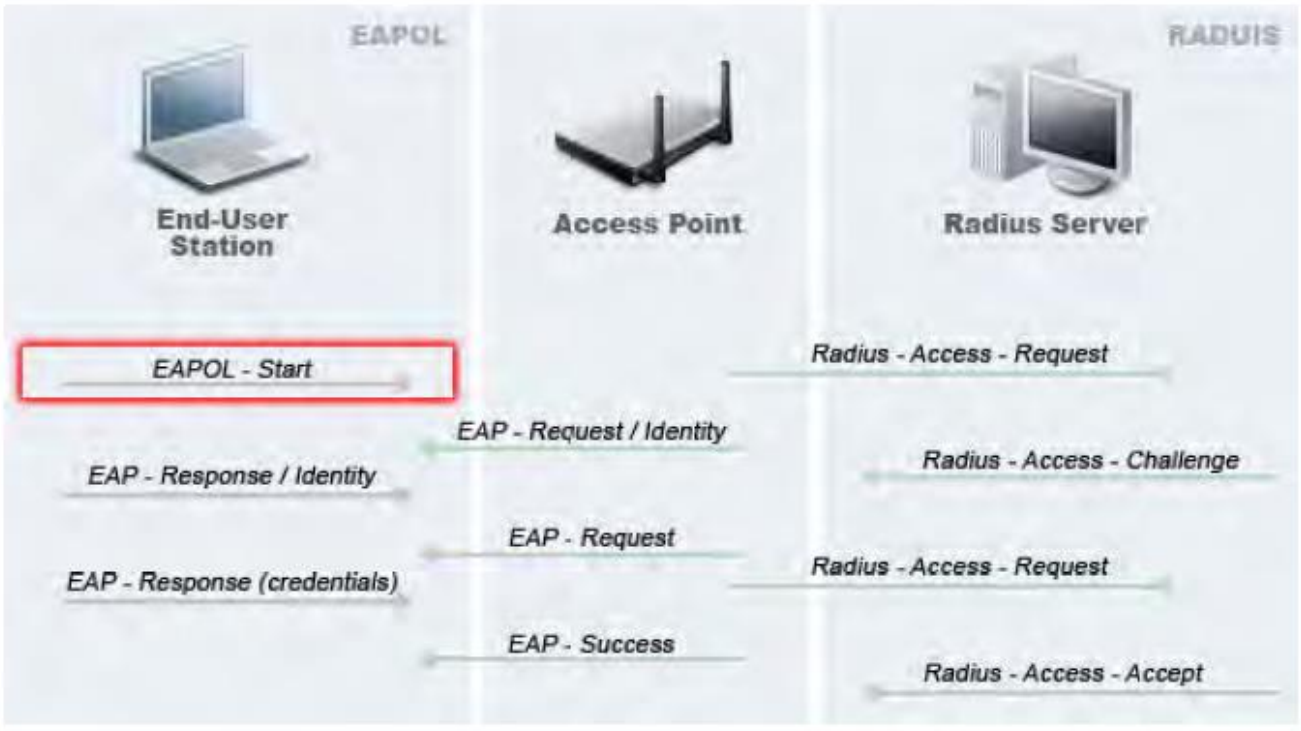
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает эту форму DoS-атаки, отслеживая состояния аутентификации 802.1x. При срабатывании сигнала тревоги будут идентифицированы атакованные клиент и точка доступа. Офицер безопасности WLAN может войти в точку доступа, чтобы проверить текущее состояние таблицы подключений, или использовать активные инструменты AirMagnet (Diagnostics, DHCP, Ping) для тестирования беспроводных услуг, предоставляемых этой точкой доступа.

Denial-of-Service Attack: EAPOL-Start Attack (Атака «отказ в обслуживании»: Атака EAPOL-Start)

Описание сигнала тревоги и возможные причины

Стандарт IEEE 802.1x определяет протокол аутентификации с использованием EAP (Extensible Authentication Protocol – протокол расширенной аутентификации) в локальных сетях или EAPOL. Для начала транзакции аутентификации протокол 802.1x начинается с кадра EAPOL-Start. Точка доступа отвечает на кадр EAPOL-Start запросом EAP-Identity-Request и выделением некоторых внутренних ресурсов.



End-User Station	Станция конечного пользователя
Access Point	Точка доступа
Radius Server	Сервер Radius
EAPOL– Start	EAPOL – Старт
Radius –Access – Request	Radius – Доступ – Запрос
EAP-Request/Identity	EAP-Запрос/Идентификатор

EAP-Response/Identity	EAP-Ответ/Идентификатор
Radius –Access – Challenge	Radius – Доступ – Требование
EAP-Request	EAP-Запрос
EAP-Response (credentials)	EAP-Ответ (учетные данные)
Radius –Access – Request	Radius – Доступ – Запрос
EAP-Success	EAP-Успешно
Radius –Access – Accept	Radius – Доступ – Принято

Злоумышленник лавинно рассылает кадры 802.1x EAPOL-Start для исчерпания ресурсов точки доступа

Злоумышленник может попытаться вывести точку доступа из строя, зафлудив её кадрами EAPOL-Start, чтобы исчерпать внутренние ресурсы. Когда у точки доступа больше не остается внутренних ресурсов, пользователи не смогут подключаться к ней, чем инициируется «отказ в обслуживании».

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает эту форму атаки типа «отказ в обслуживании», отслеживая переход состояния аутентификации 802.1x и сигнатуру конкретной атаки. При срабатывании сигнала тревоги будут идентифицированы атакованный клиент и точка доступа. Офицер безопасности сети WLAN может войти в точку доступа, чтобы проверить текущее состояние таблицы подключений, или использовать активные инструменты AirMagnet (Diagnostics, DHCP, Ping) для тестирования беспроводных услуг, предоставляемых этой точкой доступа.

Denial-of-Service Attack: EAP ID Flood Attack (Атака типа «отказ в обслуживании»: Флуд-атака EAP ID)

Описание сигнала тревоги и возможные причины

Стандарты IEEE 802.1x и IETF RFC 2284 определяют формат заголовка пакета EAP следующим образом:

Octet number	Номер октета
Code	Код
Identifier	Идентификатор
Length	Длина
Data	Данные

Формат заголовка пакета 802.1x EAP - поле идентификатора имеет длину 1 байт

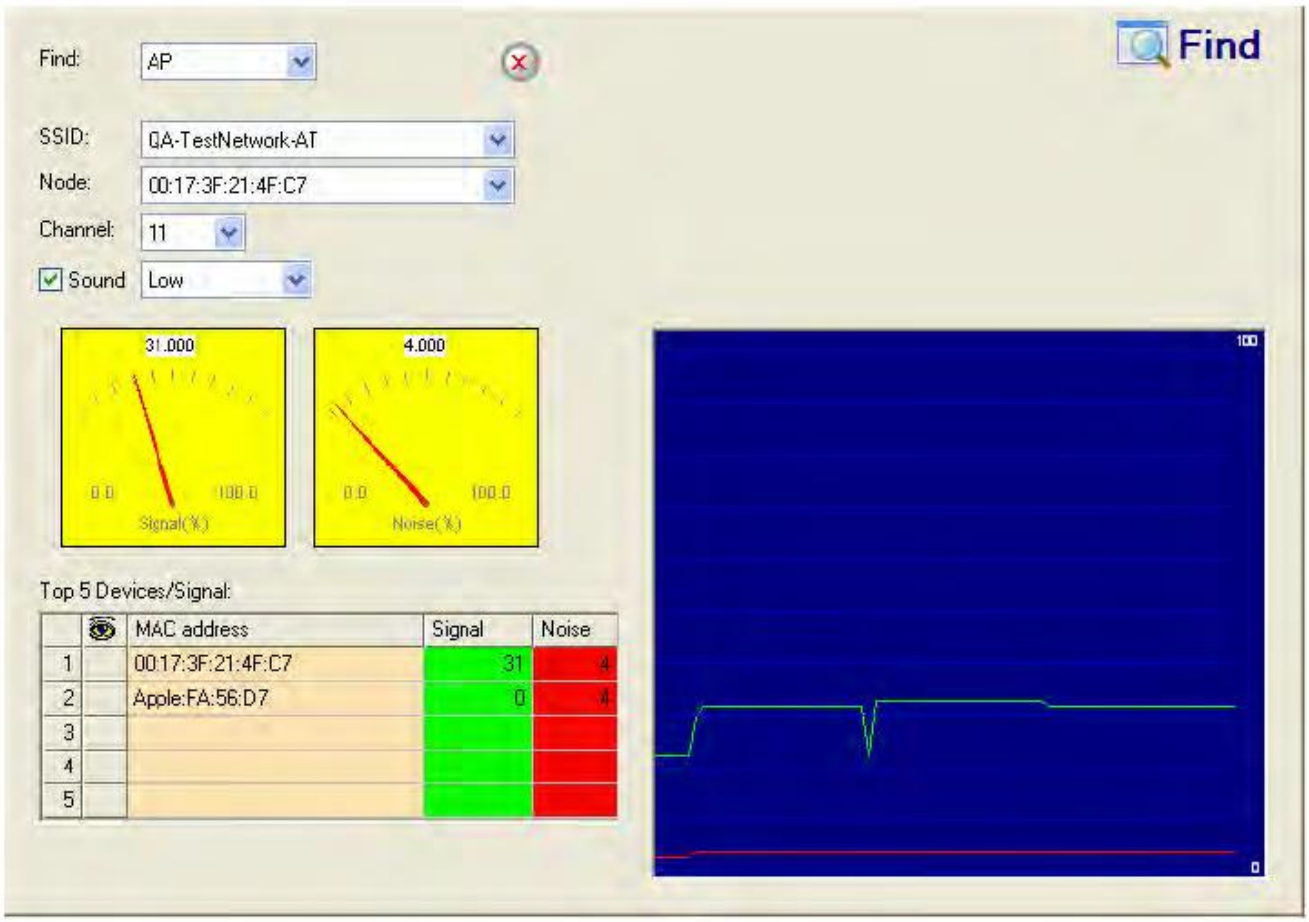
Поле идентификатора имеет длину один октет и позволяет сопоставлять ответы с запросами. Поле идентификатора (Identifier) и системный порт (System Port) (то есть, подключение 802.11) вместе однозначно идентифицируют обмен при аутентификации. Таким образом, использование поля идентификатора в один октет дает ограничение в 256 аутентификаций на системный порт.

Злоумышленник может попытаться отключить возможность аутентификации 802.1x на точке доступа, используя пространство идентификатора EAP (0–255). Поскольку идентификатор EAP должен быть уникальным только в рамках подключения 802.11, точка доступа не должна блокировать дальнейшие

соединения после того, как пространство идентификатора будет исчерпано. Эта атака эффективна только на точки доступа, которые реализуют идентификатор EAP в качестве общесистемного параметра (в отличие от параметра подключения 802.11).

Решение AirMagnet

Используйте инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer, чтобы найти устройство и предпринять соответствующие шаги для его удаления из беспроводной среды. Смотрите рисунок ниже.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Denial-of-Service Attack: Premature EAP-Success Attack (Атака типа «отказ в обслуживании»: Атака с преждевременным пакетом EAP-Success)

Описание сигнала тревоги и возможные причины

Стандарт IEEE 802.1x определяет протокол аутентификации с использованием EAP (Extensible Authentication Protocol – протокол расширенной аутентификации) в локальных сетях или EAPOL. Для начала транзакции аутентификации протокол 802.1x начинается с кадра EAPOL-Start. Когда обмен пакетами аутентификации 802.1x с внутренним сервером RADIUS завершается, точка доступа отправляет клиенту кадр EAP-Success, означающий успешную аутентификацию. Смотрите показанный ниже обмен протоколами:

End-User Station	Станция конечного пользователя
Access Point	Точка доступа
Radius Server	Сервер Radius
EAPOL– Start	EAPOL – Старт
Radius –Access – Request	Radius – Доступ – Запрос
EAP-Request/Identity	EAP-Запрос/Идентификатор
EAP-Response/Identity	EAP-Ответ/Идентификатор
Radius –Access – Challenge	Radius – Доступ – Требование
Spoofed EAP-Success	Поддельный пакет EAP-Success
EAP-Request	EAP-Запрос
Radius – Access – Request	Radius – Доступ – Запрос
EAP-Response (credentials)	EAP-Ответ (учетные данные)
EAP-Success	EAP-Успешно
Radius –Access – Accept	Radius – Доступ – Принято

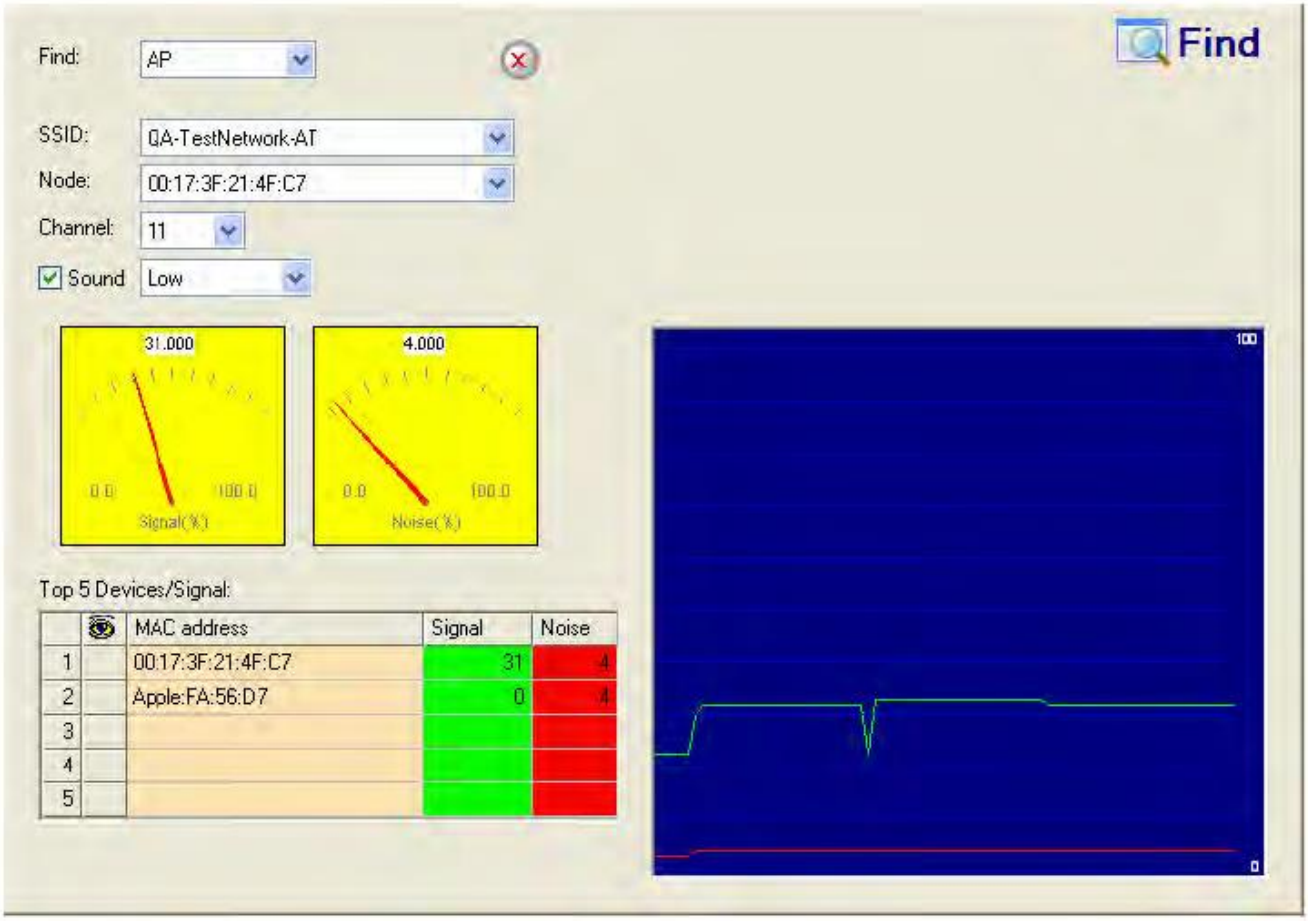
Злоумышленник подделывает заранее подготовленные кадры EAP-Success от точки доступа до завершения аутентификации

Спецификация IEEE 802.1X запрещает клиенту активировать свой интерфейс, если не была завершена требуемая взаимная аутентификация. Это позволяет правильно реализованной клиентской станции 802.1x избежать введения в заблуждение поддельной точкой доступа, отправляющей преждевременные пакеты EAP-Success для обхода процесса взаимной аутентификации.

Злоумышленник может предотвратить запуск клиентского интерфейса (следовательно, вызвать состояние «отказ в обслуживании») путем непрерывной подмены заранее подготовленных кадров EAP-Success, передаваемых от точки доступа клиенту. Это нарушит состояние аутентификации на клиенте, как описано в предыдущем абзаце.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает эту форму DoS-атаки, отслеживая поддельные заранее подготовленные кадры EAP-Success и состояния аутентификации 802.1x для каждой клиентской станции и точки доступа. Пользователь может использовать инструмент Find (Найти) приложения AirMagnet Wi-Fi Analyzer, чтобы найти устройство и предпринять соответствующие шаги для его удаления из беспроводной среды.

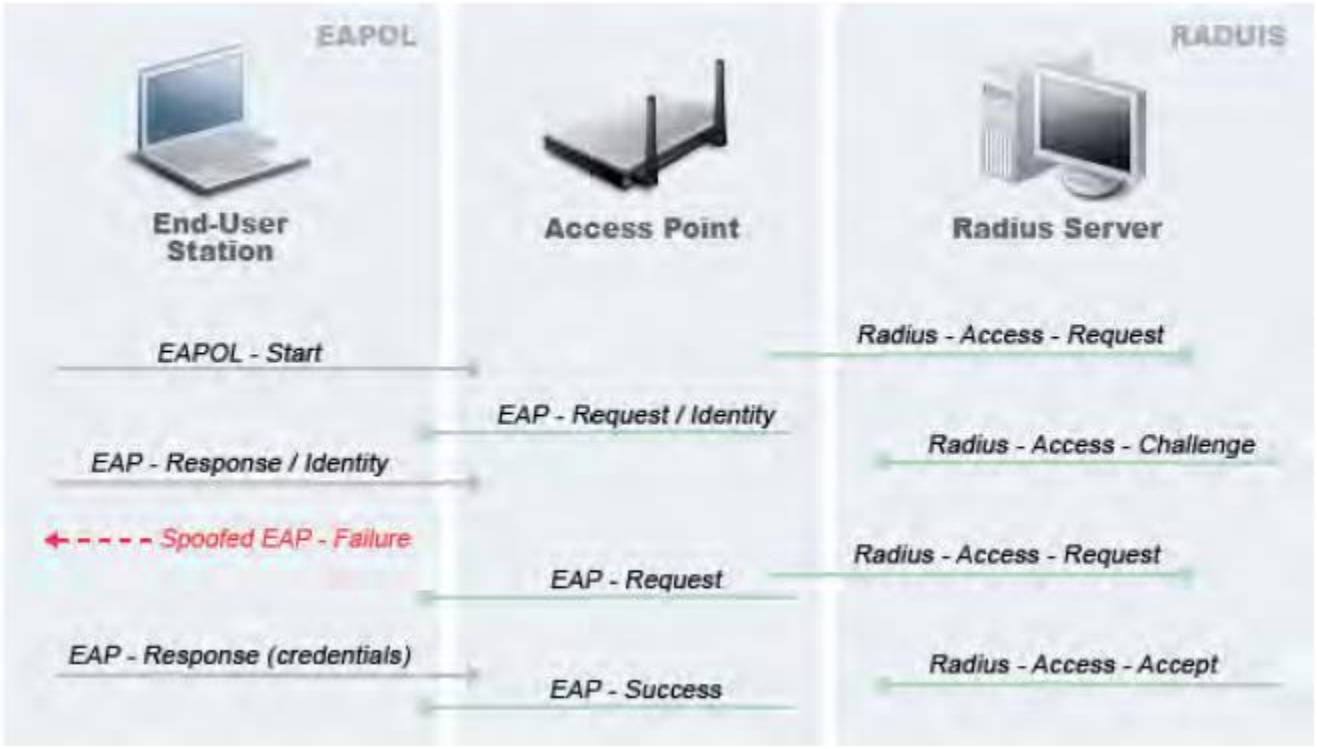


Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Denial-of-Service Attack: Premature EAP-Failure Attack (Атака типа «отказ в обслуживании: Атака с преждевременным пакетом EAP-Failure)

Описание сигнала тревоги и возможные причины

Стандарт IEEE 802.1x определяет протокол аутентификации с использованием EAP (Extensible Authentication Protocol – протокол расширенной аутентификации) в локальных сетях или EAPOL. Для начала транзакции аутентификации протокол 802.1x начинается с кадра EAPOL-Start. Когда обмен пакетами аутентификации 802.1x с внутренним сервером RADIUS завершается, точка доступа отправляет клиенту кадр EAP-Success или EAP-Failure, чтобы обозначить успешную или неудачную аутентификацию. Смотрите показанный ниже обмен протоколами:



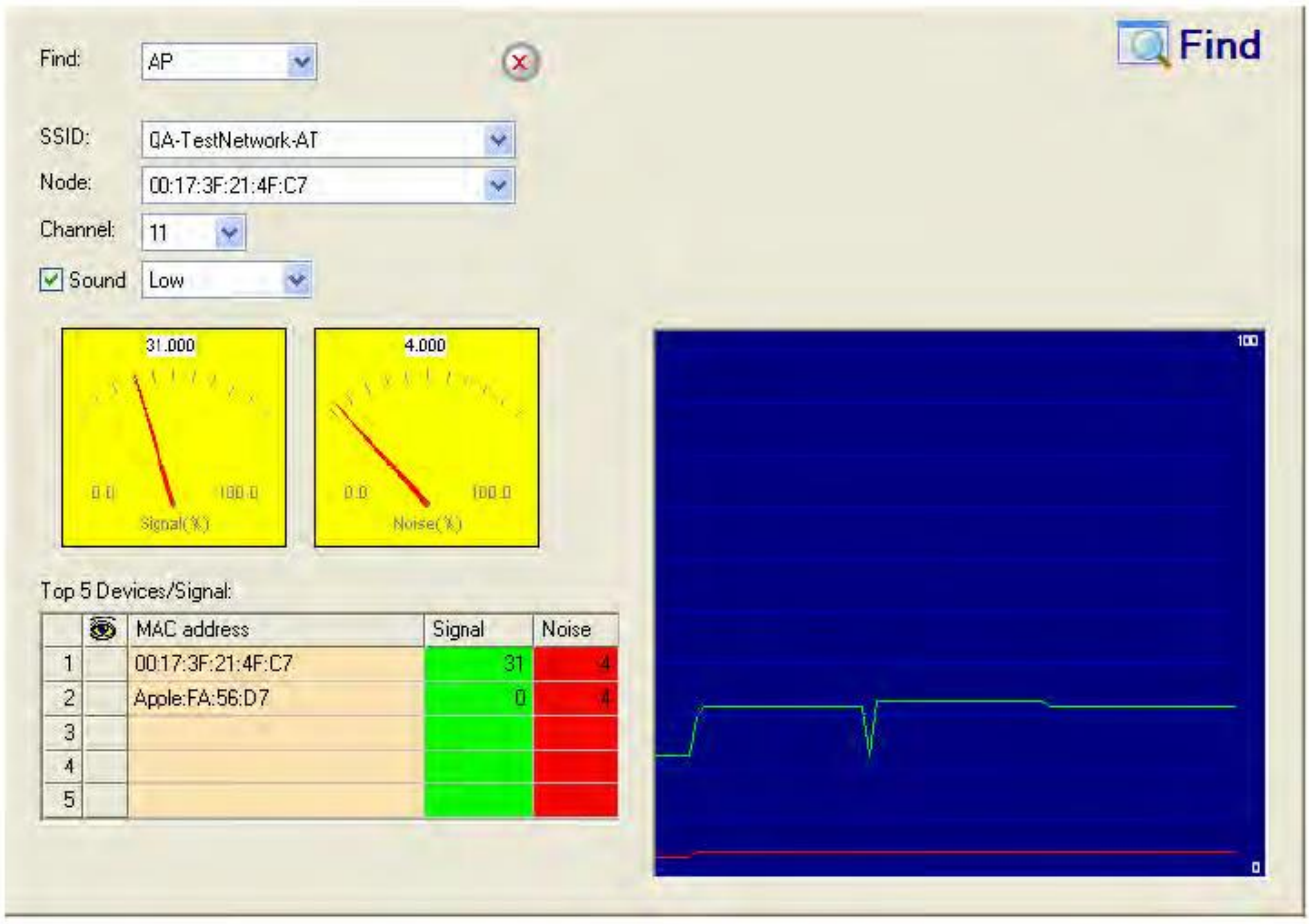
End-User Station	Станция конечного пользователя
Access Point	Точка доступа
Radius Server	Сервер Radius
EAPOL– Start	EAPOL – Старт
Radius –Access – Request	Radius – Доступ – Запрос
EAP-Request/Identity	EAP-Запрос/Идентификатор
EAP-Response/Identity	EAP-Ответ/Идентификатор
Radius –Access – Challenge	Radius – Доступ – Требование
Spoofed EAP-Failure	Поддельный пакет EAP-Failure
EAP-Request	EAP-Запрос
Radius –Access – Request	Radius – Доступ – Запрос
EAP-Response (credentials)	EAP-Ответ (учетные данные)
EAP-Success	EAP-Успешно
Radius –Access – Accept	Radius – Доступ – Принято

Злоумышленник подделывает заранее подготовленные кадры EAP-Failure от точки доступа до завершения аутентификации

Спецификация IEEE 802.1X запрещает клиенту активировать свой интерфейс, если не была завершена требуемая взаимная аутентификация. Это позволяет правильно реализованной клиентской станции 802.1x избежать введения в заблуждение поддельной точкой доступа, отправляющей преждевременные пакеты EAP-Success для обхода процесса взаимной аутентификации.
Злоумышленник может предотвратить запуск клиентского интерфейса (следовательно, вызвать состояние «отказ в обслуживании») путем непрерывной подмены заранее подготовленных кадров EAP-Failure, передаваемых от точки доступа клиенту. Это нарушит состояние аутентификации на клиенте, как описано в предыдущем абзаце.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает эту форму DoS-атаки, отслеживая поддельные заранее подготовленные кадры EAP-Failure и состояния аутентификации 802.1x для каждой клиентской станции и точки доступа. Пользователь может использовать инструмент Find (Найти) приложения AirMagnet Wi-Fi Analyzer, чтобы найти устройство и предпринять соответствующие шаги для его удаления из беспроводной среды.



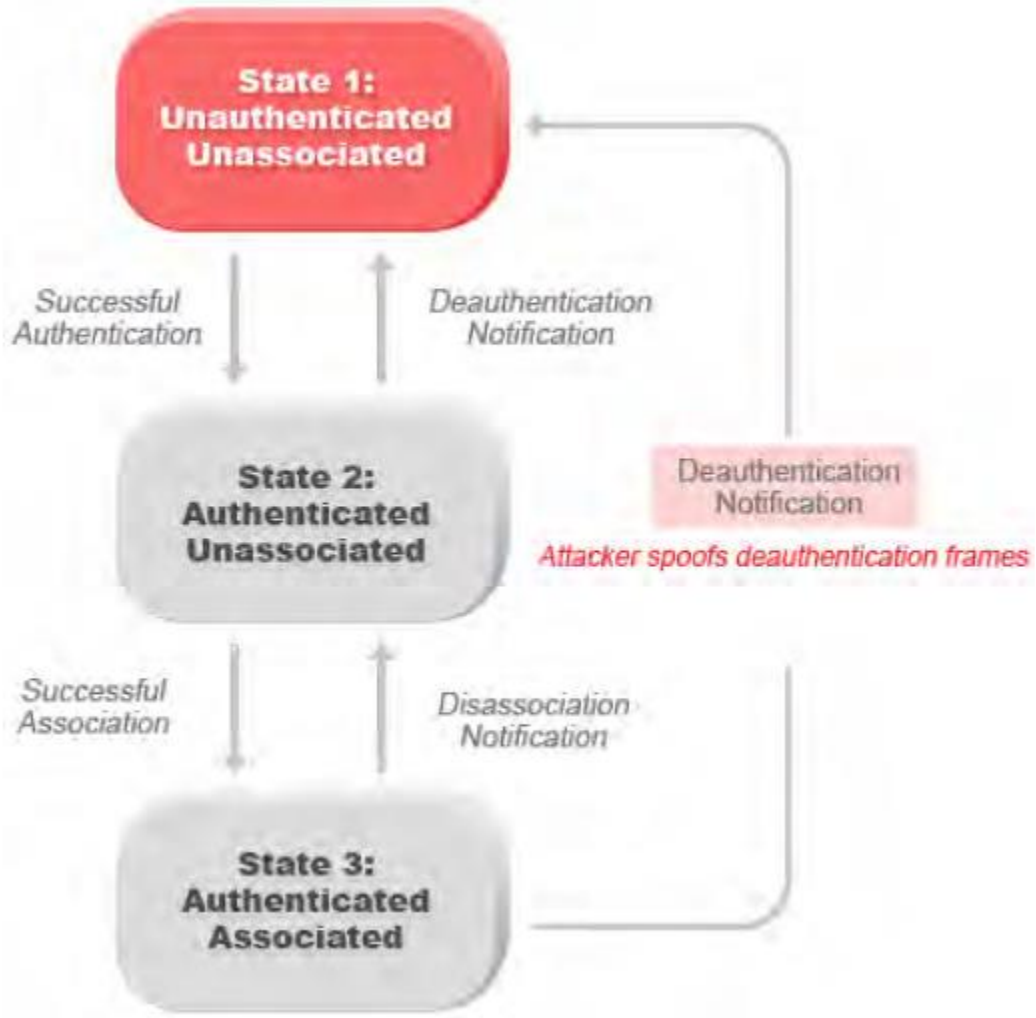
Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Denial-of-Service Attack: De-Authentication Broadcast (Атака типа «отказ в обслуживании»: Рассылка кадра деаутентификации)

Возможные инструменты атаки: WLAN Jack, Void11, Hunter Killer, AirForge

Описание сигнала тревоги и возможные причины

Для отслеживания аутентификации станции и проверки статуса ее подключения IEEE 802.11 задает машину состояний клиента. Беспроводные клиенты и точки доступа реализуют такую машину состояний (смотрите рисунок ниже) на основе стандарта IEEE. Успешно подключенная клиентская станция для продолжения беспроводной связи должна оставаться в Состоянии 3. Клиентская станция в Состоянии 1 или Состоянии 2 не может участвовать в процессе передачи данных по сети WLAN до тех пор, пока она не будет аутентифицирована и подключена для достижения Состояния 3.



State 1: …	Состояние 1: Аутентификация не пройдена, нет соединения
Successful Authentication	Успешная аутентификация
Deauthentication Notification	Извещение о деаутентификации
State 2:…	Состояние 2: Аутентификация пройдена, нет соединения
Attacker spoofs deauthentication frames	Злоумышленник фабрикует кадры деаутентификации
Successful Association	Успешное подключение
Diassociation Notification	Извещение о разъединении
State 3:…	Состояние 3: Аутентификация пройдена, соединение установлено

Злоумышленник подделывает кадры деаутентификации 802.11 от точки доступа к клиентской станции, чтобы перевести клиента в состояние 1

Форма атаки типа «отказ в обслуживании» направлена на отправку всех клиентов точки доступа в несвязанное/неаутентифицированное состояние 1 путем подмены кадров деаутентификации от точки доступа на широковещательный адрес. При современной реализации клиентского адаптера эта форма атаки очень эффективна и быстра с точки зрения нарушения работы беспроводных служб против нескольких клиентов. Как правило, клиентские станции повторно подключаются и повторно аутентифицируются для восстановления обслуживания до тех пор, пока злоумышленник не отправит еще один кадр деаутентификации.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer определяет эту форму DoS-атаки, обнаруживая поддельные кадры деаутентификации и отслеживая состояния аутентификации и подключения клиента. При срабатывании сигнала тревоги будет идентифицирована атакованная точка доступа. Аналитик безопасности WLAN может войти в точку доступа, чтобы проверить текущее состояние таблицы подключения, или

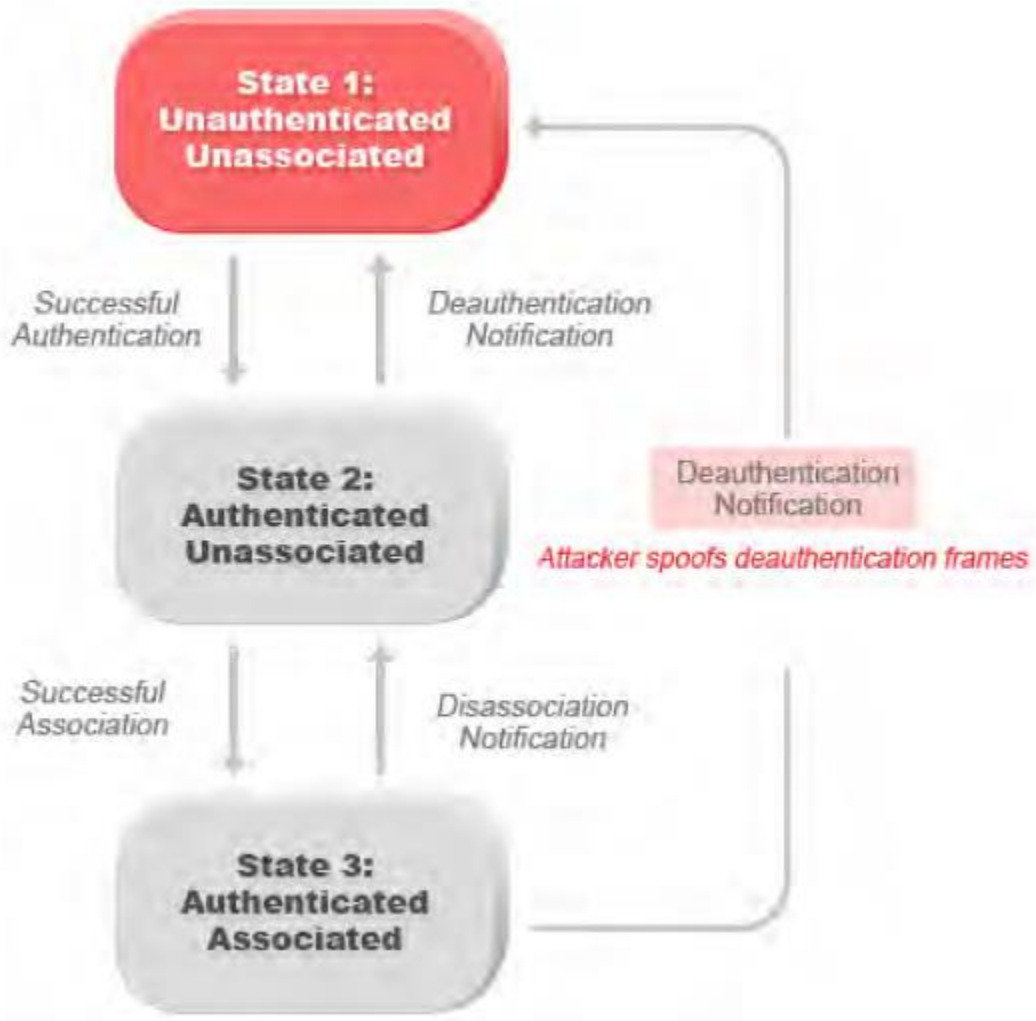
использовать активные инструменты приложения AirMagnet Wi-Fi Analyzer (Diagnostics, DHCP, Ping) для тестирования беспроводных услуг, предоставляемых этой точкой доступа.

Denial-of-Service Attack: De-Authentication Flood (Атака типа «отказ в обслуживании»: Флуд деаутентификации)

Возможные инструменты атаки: WLAN Jack, Void11, AirForge

Описание сигнала тревоги и возможные причины

Для отслеживания аутентификации станции и проверки статуса ее подключения IEEE 802.11 задает машину состояний клиента. Беспроводные клиенты и точки доступа реализуют такую машину состояний (смотрите рисунок ниже) на основе стандарта IEEE. Успешно подключенная клиентская станция для продолжения беспроводной связи должна оставаться в Состоянии 3. Клиентская станция в Состоянии 1 или Состоянии 2 не может участвовать в процессе передачи данных по сети WLAN до тех пор, пока она не будет аутентифицирована и подключена для достижения Состояния 3.



State 1: …	Состояние 1: Аутентификация не пройдена, нет соединения
Successful Authentication	Успешная аутентификация
Deauthentication Notification	Извещение о деаутентификации
State 2:…	Состояние 2: Аутентификация пройдена, нет соединения
Attacker spoofs deauthentication frames	Злоумышленник фабрикует кадры деаутентификации
Successful Association	Успешное подключение
Diassociation Notification	Извещение о разъединении
State 3:…	Состояние 3: Аутентификация пройдена, соединение установлено

Злоумышленник подделывает кадры деаутентификации 802.11 от точки доступа к клиентской станции, чтобы перевести клиента в состояние 1

Форма атаки типа «отказ в обслуживании» направлена на отправку клиента точки доступа в несвязанное/неаутентифицированное состояние 1 путем подмены кадров деаутентификации от точки доступа на конкретный адрес. При современной реализации клиентского адаптера эта форма атаки очень эффективна и быстра с точки зрения нарушения работы беспроводных служб против клиента. Как правило, клиентские станции повторно подключаются и повторно аутентифицируются для восстановления обслуживания до тех пор, пока злоумышленник не отправит еще один кадр деаутентификации. Злоумышленник будет многократно подделывать кадры деаутентификации, чтобы не допустить обслуживания всех клиентов.

Решение AirMagnet

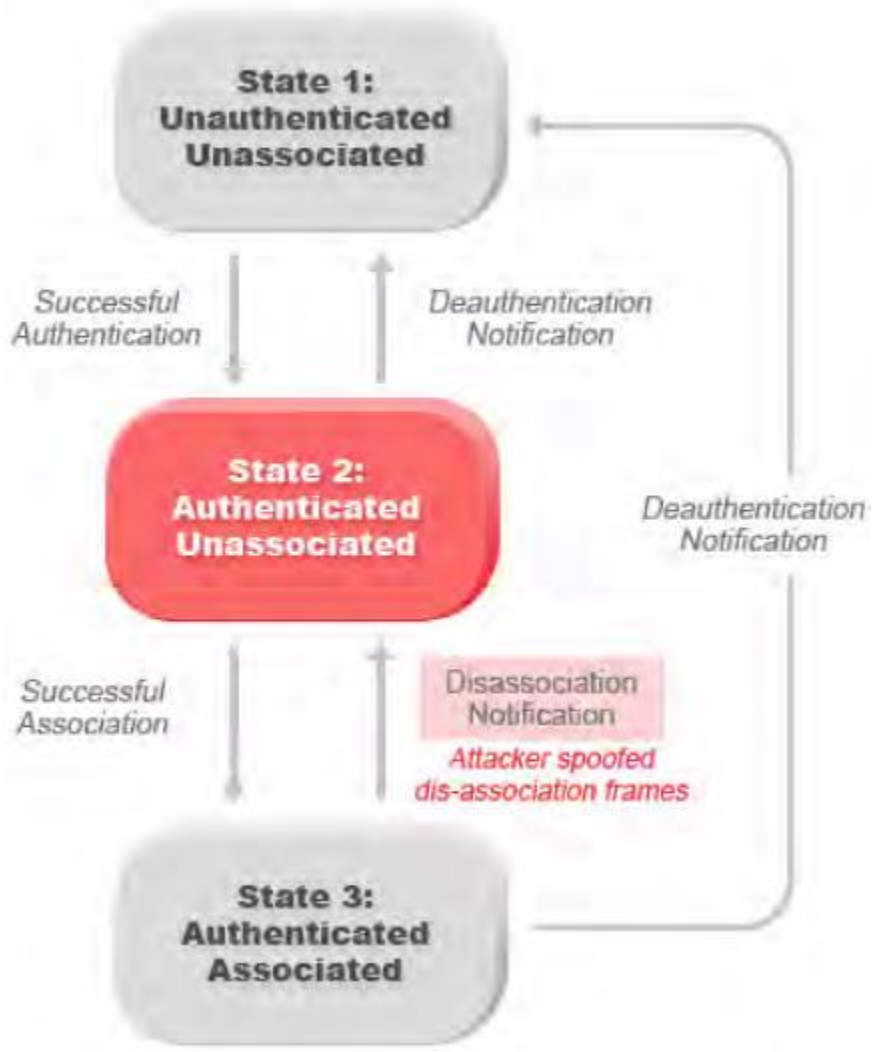
Приложение AirMagnet WiFi Analyzer определяет эту форму DoS-атаки, обнаруживая поддельные кадры деаутентификации и отслеживая состояния аутентификации и подключения клиента. При срабатывании сигнала тревоги будет идентифицирована атакованная точка доступа и клиент. Аналитик безопасности WLAN может войти в точку доступа, чтобы проверить текущее состояние таблицы подключения, или использовать активные инструменты приложения AirMagnet Wi-Fi Analyzer (Diagnostics, DHCP, Ping) для тестирования беспроводных услуг, предоставляемых этой точкой доступа.

Denial-of-Service Attack: Disassociation Broadcast (Атака типа «отказ в обслуживании»: Рассылка кадра отключения)

Возможные инструменты атаки: ESSID Jack, WLAN Jack

Описание сигнала тревоги и возможные причины

Для отслеживания аутентификации станции и проверки статуса ее подключения IEEE 802.11 задает машину состояний клиента. Беспроводные клиенты и точки доступа реализуют такую машину состояний (смотрите рисунок ниже) на основе стандарта IEEE. Успешно подключенная клиентская станция для продолжения беспроводной связи должна оставаться в Состоянии 3. Клиентская станция в Состоянии 1 или Состоянии 2 не может участвовать в процессе передачи данных по сети WLAN до тех пор, пока она не будет аутентифицирована и подключена для достижения Состояния 3.



State 1: …	Состояние 1: Аутентификация не пройдена, нет соединения
Successful Authentication	Успешная аутентификация
Deauthentication Notification	Извещение о деаутентификации
State 2:…	Состояние 2: Аутентификация пройдена, нет соединения
Successful Association	Успешное подключение
Diassociation Notification	Извещение о разъединении
Attacker spoofed…	Злоумышленник фабрикует кадры отключения
State 3:…	Состояние 3: Аутентификация пройдена, соединение установлено

Злоумышленник подменяет кадры отключения 802.11, передаваемые от точки доступа на широковещательный адрес, чтобы заставить всех клиентов перейти в состояние 2

Данная форма атаки типа «отказ в обслуживании» направлена на перевод клиента точки доступа в состояние 2 (клиент аутентифицирован, но не подключен) путем подмены кадров отключения от точки доступа на широковещательный адрес (всем клиентам). В современной реализации клиентских адаптеров эта форма атаки очень эффективна и быстра с точки зрения нарушения работы беспроводных служб для множества клиентов. Как правило, клиентские станции повторно подключаются для восстановления обслуживания до тех пор, пока злоумышленник не отправит еще один кадр отключения. Злоумышленник будет многократно подделывать кадры отключения, чтобы не допустить обслуживания всех клиентов.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer определяет эту форму DoS-атаки, обнаруживая поддельные кадры отключения и отслеживая состояния аутентификации и подключения клиента. При срабатывании сигнала тревоги будет идентифицирована атакованная точка доступа. Специалист по безопасности сети WLAN может войти в точку доступа, чтобы проверить текущее состояние таблицы подключения, или

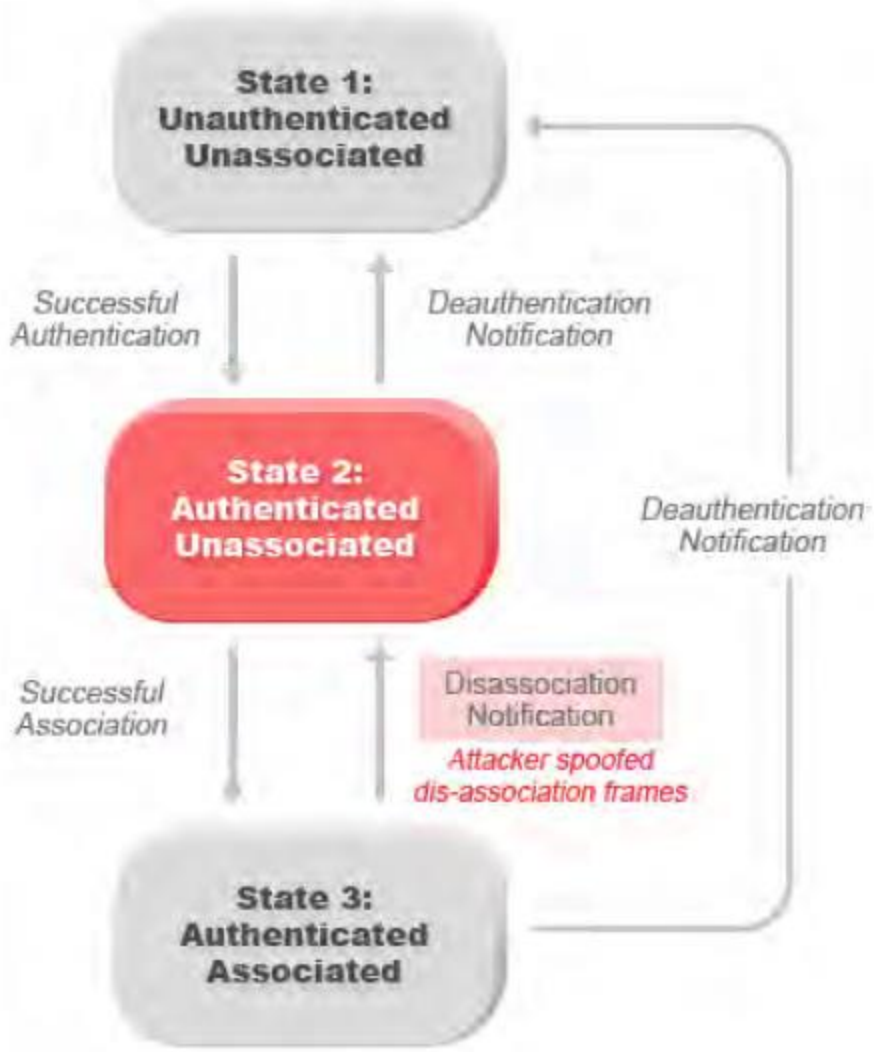
использовать активные инструменты приложения AirMagnet Wi-Fi Analyzer (Diagnostics, DHCP, Ping) для тестирования беспроводных услуг, предоставляемых этой точкой доступа.

Denial-of-Service Attack: Disassociation Flood (Атака типа «отказ в обслуживании»: Флуд кадра отключения)

Возможные инструменты атаки: ESSID Jack, WLAN Jack

Описание сигнала тревоги и возможные причины

Для отслеживания аутентификации станции и проверки статуса ее подключения IEEE 802.11 задает машину состояний клиента. Беспроводные клиенты и точки доступа реализуют такую машину состояний (смотрите рисунок ниже) на основе стандарта IEEE. Успешно подключенная клиентская станция для продолжения беспроводной связи должна оставаться в Состоянии 3. Клиентская станция в Состоянии 1 или Состоянии 2 не может участвовать в процессе передачи данных по сети WLAN до тех пор, пока она не будет аутентифицирована и подключена для достижения Состояния 3.



State 1: …	Состояние 1: Аутентификация не пройдена, нет соединения
Successful Authentication	Успешная аутентификация
Deauthentication Notification	Извещение о деаутентификации
State 2:…	Состояние 2: Аутентификация пройдена, нет соединения
Successful Association	Успешное подключение
Diassociation Notification	Извещение о разъединении
Attacker spoofed…	Злоумышленник фабрикует кадры отключения
State 3:…	Состояние 3: Аутентификация пройдена, соединение установлено

Злоумышленник подменяет кадры отключения 802.11, передаваемые от точки доступа на клиентскую станцию, чтобы перевести клиента в состояние 2

Данная форма атаки типа «отказ в обслуживании» направлена на перевод клиента точки доступа в состояние 2 (клиент аутентифицирован, но не подключен) путем подмены кадров отключения, передаваемых от точки доступа клиенту. В современной реализации клиентских адаптеров эта форма атаки очень эффективна и быстра с точки зрения нарушения работы беспроводных служб для данного клиента. Как правило, клиентские станции повторно подключаются для восстановления обслуживания до тех пор, пока злоумышленник не отправит еще один кадр отключения. Злоумышленник будет многократно подделывать кадры отключения, чтобы не допустить обслуживания этого клиента.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer определяет эту форму DoS-атаки, обнаруживая поддельные кадры отключения и отслеживая состояния аутентификации и подключения клиента. При срабатывании сигнала тревоги будет идентифицирована атакованная точка доступа. Специалист по безопасности сети WLAN может войти в точку доступа, чтобы проверить текущее состояние таблицы подключения, или использовать активные инструменты приложения AirMagnet Wi-Fi Analyzer (Diagnostics, DHCP, Ping) для тестирования беспроводных услуг, предоставляемых этой точкой доступа.

Denial-of-Service Attack: RF Jamming Attack (Атака типа «отказ в обслуживании»: Атака радиочастотных помех)

Описание сигнала тревоги и возможные причины

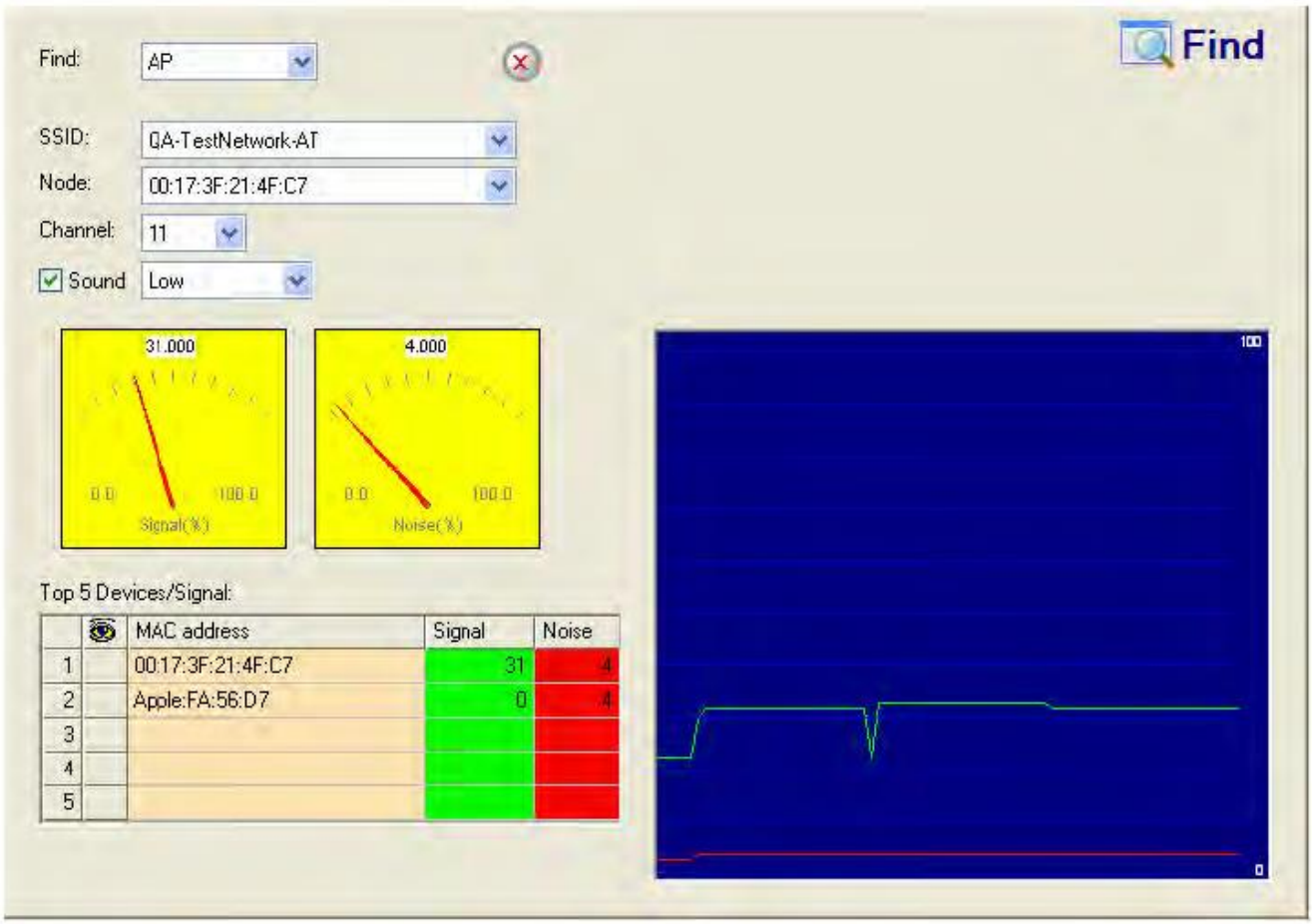
Надежность и эффективность сети WLAN зависят от качества радиочастотной среды. Будь то 802.11b/g в частотном диапазоне 2,4 ГГц или 802.11a в частотном диапазоне 5 ГГц, все они подвержены влиянию радиочастотного шума. Использующий эту уязвимость WLAN злоумышленник может осуществлять DoS-атаки двух типов:

- Нарушение работы сети WLAN: В нелицензируемом частотном диапазоне 2,4 ГГц атака может быть непреднамеренной. Беспроводный телефон, устройства Bluetooth, микроволновая печь, беспроводная видеокамера системы наблюдения или радионяня могут излучать радиочастотную энергию, нарушая работу сети WLAN. Вредоносные атаки позволяют манипулировать мощностью радиочастотных сигналов в диапазоне 2,4 ГГц или 5 ГГц с помощью направленной антенны с высоким коэффициентом усиления, позволяющей производить атаки на расстоянии. При затухании в свободном пространстве и внутри помещения, глушитель мощностью 1 киловатт на расстоянии 100 метров от здания может воздействовать на офисную зону на глубину 15 – 30 метров. Тот же глушитель мощностью 1 киловатт, расположенный внутри здания, может нарушить работу сети в радиусе 60 метров. Во время проведения подобной атаки устройства в целевой зоне WLAN не будут получать беспроводные услуги.
- Физическое повреждение оборудования точки доступа: Злоумышленник, использующий передатчик с высокой выходной мощностью и направленной антенной с высоким коэффициентом усиления в 30 метрах от точки доступа, может передавать высокочастотную мощность, достаточную для повреждения электроники точки доступа, что приведет к ее полному отключению. Было продемонстрировано, что такие пушки HERF (высокоэнергетические радиочастотные) не только работают, но и стоят очень недорого.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает непрерывный радиочастотный шум выше определенного порогового значения, трактуя его как потенциальную атаку радиопомех. Сообщение об атаке с помощью радиочастотных помех можно дополнительно расследовать путем отслеживания источника шумов с помощью инструмента AirMagnet Find с внешней направленной антенной.

Отслеживание с помощью портативного анализатора AirMagnet на КПК источника шумов при атаке с использованием радиочастотных помех



Инструмент Find (Найти) приложения AirMagnet Wi-Fi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Dictionary Attack on EAP Methods (Атака по словарю на методы EAP)

Описание сигнала тревоги и возможные причины

Стандарт IEEE 802.1x предоставляет для аутентификации в проводных или беспроводных локальных сетях структуру EAP (Extensible Authentication Protocol – протокол расширенной аутентификации). Структура EAP позволяет гибко реализовать протокол аутентификации. Производители оборудования для беспроводных сетей, поддерживающего стандарты 802.1x или WPA, реализуют такие протоколы аутентификации, как LEAP, MD5, OTP (одноразовый пароль), TLS, TTLS и т.д. Некоторые из этих протоколов аутентификации основаны на механизме ввода имени пользователя и пароля, где имя пользователя передается в открытом виде без шифрования, а пароль используется для ответа на запросы аутентификации.

Большинство алгоритмов аутентификации на основе паролей подвержены атакам по словарю. Во время атаки по словарю злоумышленник получит имя пользователя в результате обмена по протоколу незашифрованными идентификаторами 802.1x. Затем злоумышленник пытается угадать пароль пользователя и получить доступ к сети, используя каждое «слово» в словаре наиболее часто используемых паролей или возможных комбинаций паролей. Атака по словарю основана на том факте, что пароль часто представляет собой обычное слово, имя или объединение слов или имен с такими незначительными изменениями, как одна или две цифры в конце.

Атака по словарю может активно проводиться в сети, когда злоумышленник многократно перебирает все возможные комбинации паролей. Онлайн-атаки по словарю можно предотвратить с помощью механизмов блокировки, доступных на сервере аутентификации (серверах RADIUS), которые позволяют заблокировать пользователя после определенного количества недействительных попыток входа в систему. Атака по словарю также может осуществляться в режиме офлайн, когда злоумышленник захватывает успешный обмен протоколами запроса аутентификации и затем в режиме офлайн пытается сопоставить ответ на запрос со всеми возможными комбинациями паролей. В отличие от сетевых атак, офлайн-атаки нелегко обнаружить. Использование надежной политики паролей и периодическая их замена пользователями значительно снижает эффективность офлайн-атак.

Решение AirMagnet

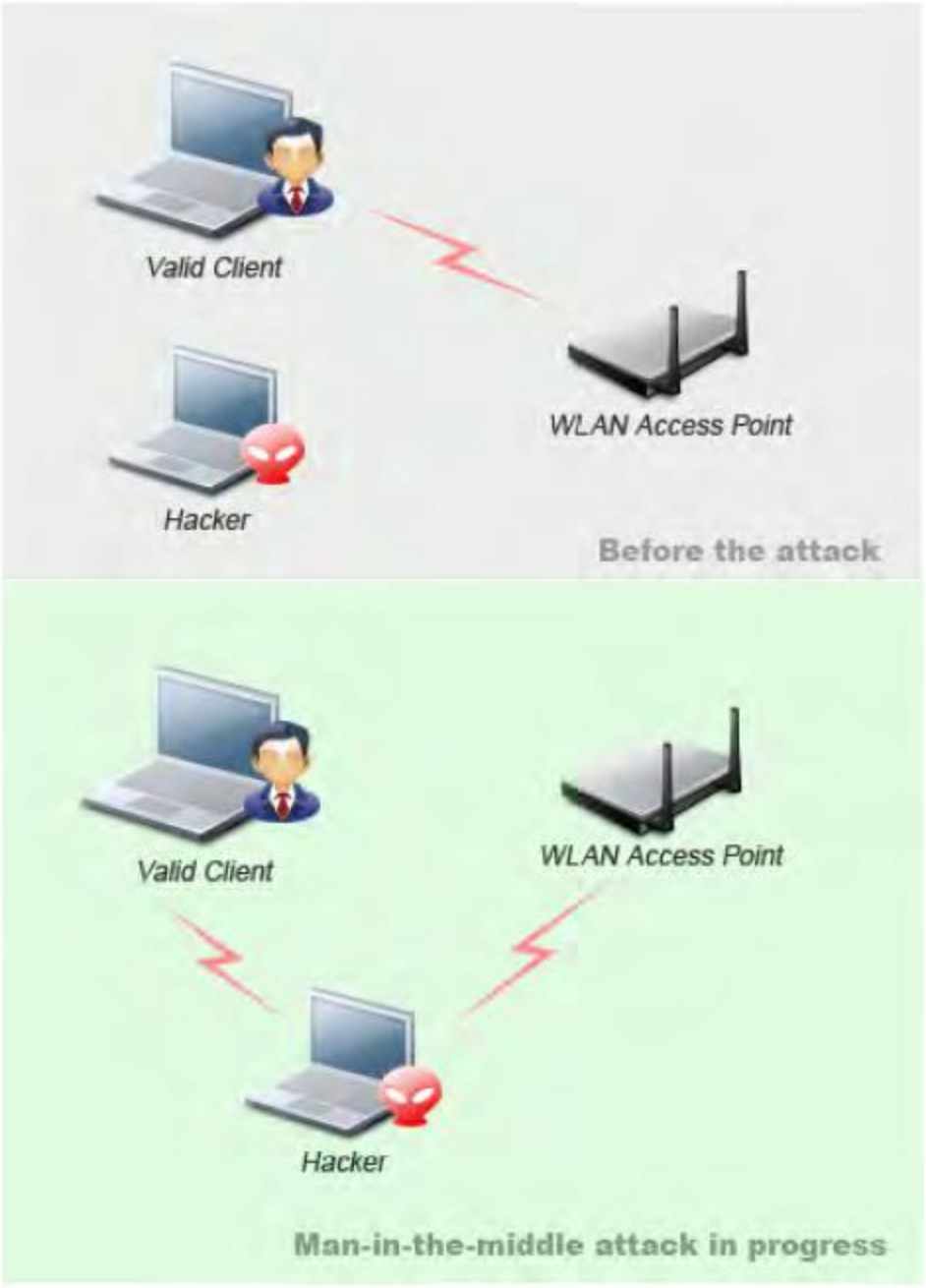
Приложение AirMagnet WiFi Analyzer обнаруживает онлайн-атаки по словарю, отслеживая обмен протоколами аутентификации 802.1x и использование идентификаторов пользователей. При обнаружении атаки по словарю сообщение приложения AirMagnet WiFi Analyzer идентифицирует имя пользователя и MAC-адрес атакующей станции. AirMagnet рекомендует переключить методы аутентификации с имени пользователя и пароля на такие зашифрованные методы аутентификации на основе туннеля, как PEAP и EAP-FAST, поддерживаемые многими производителями, включая Cisco.

Men-in-the-Middle Attack Detected (Обнаружена атака «человек посередине»)

Инструмент потенциальной атаки: Monkey Jack

Описание сигнала тревоги и возможные причины

Атака Man-in-the-Middle (MITM) является одной из наиболее распространенных атак 802.11, которая может приводить к получению хакерами конфиденциальной корпоративной и частной информации. При атаке MITM хакер может использовать анализатор беспроводной сети 802.11 и отслеживать кадры 802.11, отправляемые по беспроводной локальной сети. Захватив беспроводные кадры на этапе подключения, хакер способен получить информацию об IP- и MAC-адресах карты беспроводного клиента и точки доступа, идентификатор подключения для клиента и идентификатор SSID беспроводной сети.



Valid Client	Легитимный клиент
WLAN Access Point	Точка доступа сети WLAN
Hacker	Хакер
Before the attack	Перед атакой
Man-in-the-middle attack in progress	Осуществляется атака «человек посередине»

Часто используемая атака «человек посередине»

Наиболее часто используемый в настоящее время метод выполнения атаки «человек посередине» заключается в том, что хакер отправляет поддельные кадры отключения или деаутентификации. После этого хакерская станция подделывает MAC-адрес клиента, чтобы продолжить подключение к точке доступа. В то же время хакер устанавливает поддельную точку доступа в другом канале, чтобы поддерживать связь с клиентом. Теперь весь трафик между легитимным клиентом и точкой доступа будет проходить через станцию хакера. Одним из наиболее часто используемых инструментов атаки типа «человек посередине» является Monkey-Jack.

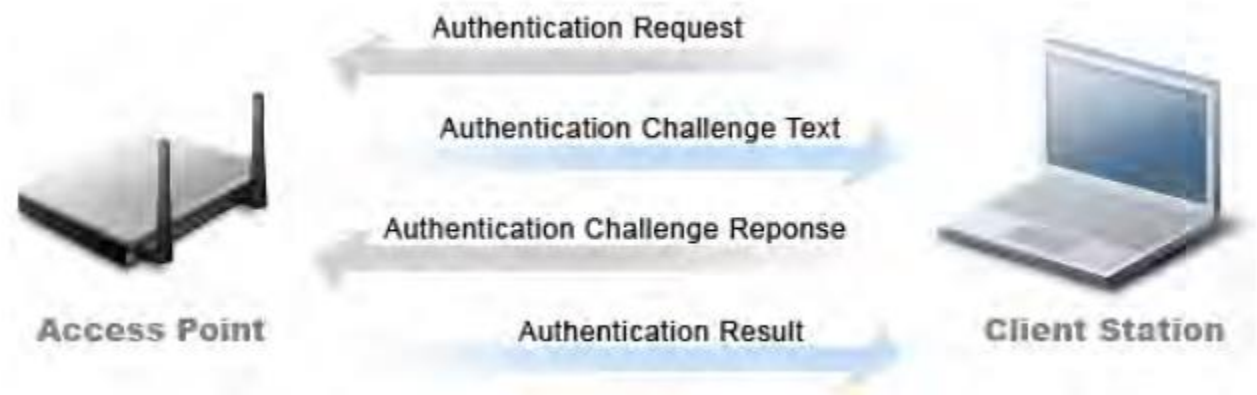
Решение AirMagnet

Для предотвращения любых атак хакеров типа «человек посередине» приложение AirMagnet WiFi Analyzer рекомендует использовать надежные механизмы шифрования и аутентификации. Одним из способов избежания подобной атаки является предотвращение подмены MAC-адресов с помощью списков исключений MAC-адресов и мониторинга среды радиочастотных каналов.

Device Using Shared Key Authentication (Устройство, использующее аутентификацию с совместно используемым ключом)

Описание сигнала тревоги и возможные причины

Для блокировки связи неавторизованных устройств WLAN с точкой доступа или станцией ad-hoc стандартом IEEE 802.11 предусмотрен протокол аутентификации с совместно используемым ключом, работающий со статическим ключом шифрования WEP. Это простой протокол обмена запросами/ответами, состоящий из показанных ниже четырех пакетов:



Authentication Request	Запрос аутентификации
Authentication Challenge Text	Текст запроса аутентификации
Authentication Challenge Request	Ответ на запрос аутентификации
Authentication Result	Результат аутентификации
Access Point	Точка доступа
Client Station	Клиентская станция

4-пакетный обмен протокола аутентификации с совместно используемым ключом

Для аутентификации между клиентом 802.11 и точкой доступа с совместно используемым ключом используется стандартный подход запроса и ответа. Запрос не зашифрован и представляет собой открытый текст. Алгоритм (не совместно используемый секретный ключ) ответа на запрос является стандартным и общеизвестным. Было доказано, что аутентификацию с совместно используемым ключом можно легко использовать в пассивной атаке путем подслушивания. Злоумышленник может использовать грубую силу для вычисления ответа на запрос в офлайн-режиме после захвата текста запроса, который является открытым. Как только совпадение найдено, злоумышленник получает совместно используемый секретный ключ. Обратитесь к документу «Your 802.11 Wireless Network has No Clothes (Ваша беспроводная сеть 802.11 без покровов)», опубликованному Университетом Мэриленда, в котором освещаются некоторые проблемы безопасности, включая уязвимость совместно используемого ключа в беспроводных локальных сетях.

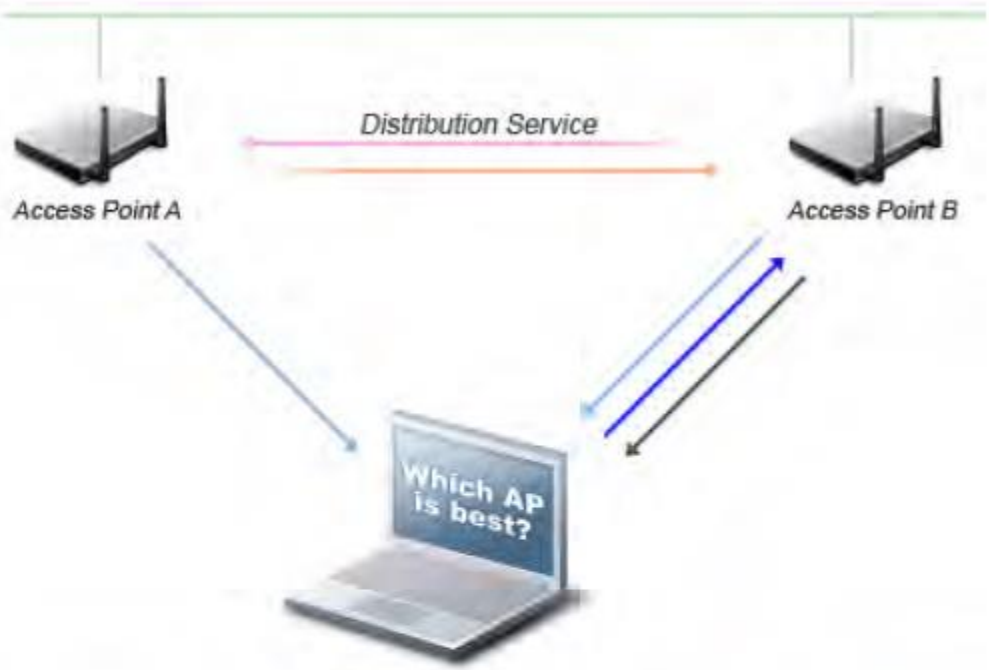
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает применение аутентификации с совместно используемым ключом и предлагает альтернативы. Многие современные предприятия развертывают сети WLAN 802.11 с использованием открытой аутентификации вместо аутентификации с совместно используемым ключом с механизмом аутентификации более высокого уровня, который обеспечивается такими методами 802.1x и EAP, как LEAP, PEAP, TLS и т.д.

Excessive Roaming or Re-Associations (Чрезмерный роуминг или повторные подключения)

Описание сигнала тревоги и возможные причины

После успешного подключения к точке доступа клиентские устройства VoWLAN начинают использовать беспроводное соединение для связи, но продолжают поиск лучших беспроводных услуг (например, другую точку доступа с более сильным сигналом, меньшими шумами канала или более высокой поддерживаемой скоростью).



Distribution Service	Услуга распределения
Access Point A (B)	Точка доступа A (B)
Which AP is best?	Какая точка доступа лучше?
1. Адаптер в настоящий момент связан с точкой доступа A, но прослушивает сигналы маяка от всех точек доступа. 2. Адаптер оценивает маяки точек доступа, выбирая лучшую из них. 3. Адаптер передает запрос на подключение на выбранную точку доступа (B). 4. Точка доступа B подтверждает подключение и регистрирует адаптер. 5. Точка доступа B информирует точку доступа A о переподключении на точку доступа B с помощью DS. 6. Точка доступа A передает буферизированные пакеты на точку доступа B и отменяет регистрацию адаптера.	

Беспроводной клиент переключается на лучшую точку доступа для обеспечения более качественной связи

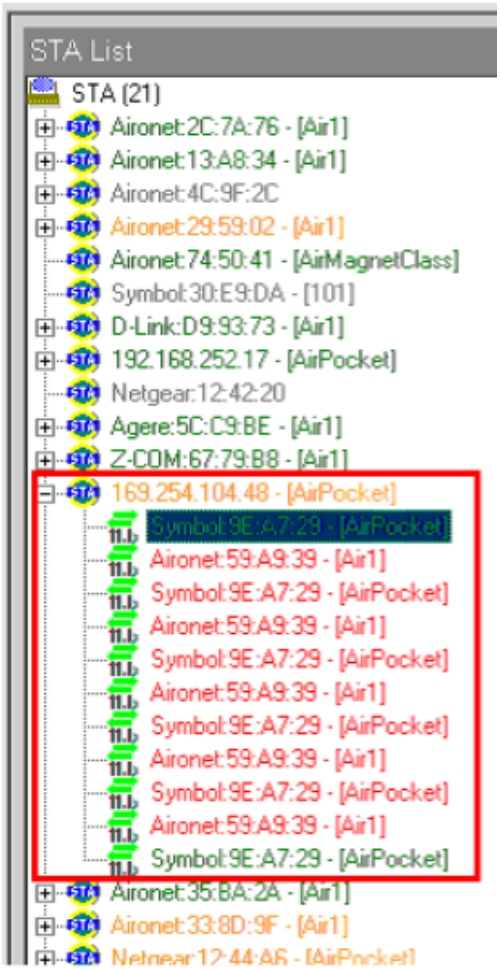
Как только определена точка доступа с лучшим обслуживанием, клиентская станция подключится к ней и разорвет соединение с исходной точкой доступа. Мобильные устройства в роуминге (телефоны VoIP и сканеры штрих-кода) WLAN часто выполняют такое повторное подключение. Благодаря более совершенным технологиям управления WLAN (например, перечисленным ниже) клиентские станции с большей вероятностью изменят подключение, чтобы приспособиться к динамической радиочастотной среде:

- Балансировка нагрузки точки доступа и распределение полосы пропускания.
- Динамический выбор канала для предотвращения радиопомех и выделенная полоса пропускания канала.
- Автоматическая регулировка выходной мощности точки доступа для оптимизации покрытия и емкости.

Все эти технологии повышают эффективность сети WLAN. Однако реализации и точная настройка, которые выполняются производителем оборудования, не соответствуют друг другу. Новые незрелые продукты могут приводить к частому повторному подключению сбитых с толку клиентских станций, что приведет к нарушению обслуживания.

Решение AirMagnet

Не ожидается, что стационарные устройства (например, беспроводные принтеры и беспроводные настольные компьютеры) будут часто повторно подключаться. Приложение AirMagnet WiFi Analyzer отслеживает чрезмерное количество повторных подключений клиентов, подсчитывая количество соединений и точек доступа. После обнаружения и получения сообщения от приложения AirMagnet WiFi Analyzer эту проблему можно дополнительно исследовать с помощью списка станций на странице Infrastructure (Инфраструктура), отображая задействованные точки доступа и характеристики сеанса (смотрите пример ниже).



Станция 169.254.104.48 переключалась между двумя точками доступа 11 раз.

Использование списка станций на странице инфраструктуры (Infrastructure) для исследования проблемы чрезмерного роуминга

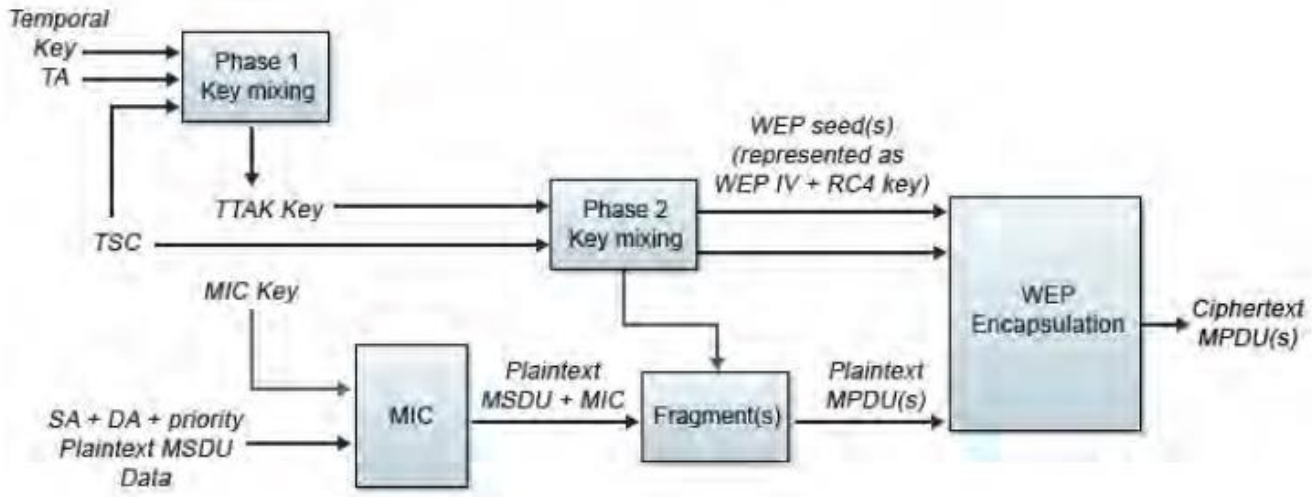
Policy – RTS frames not responded to by CTS (Политика - кадры RTS, на которые нет ответных кадров CTS)

На запрос RTS (Request-To-Send) обычно поступает ответ CTS (Clear-To-Send), а затем следует фактическая передача данных. Без приема кадра CTS станция не может передавать данные, что приводит к нарушению беспроводной связи.

Device Unprotected by TKIP (Устройство не защищено TKIP)

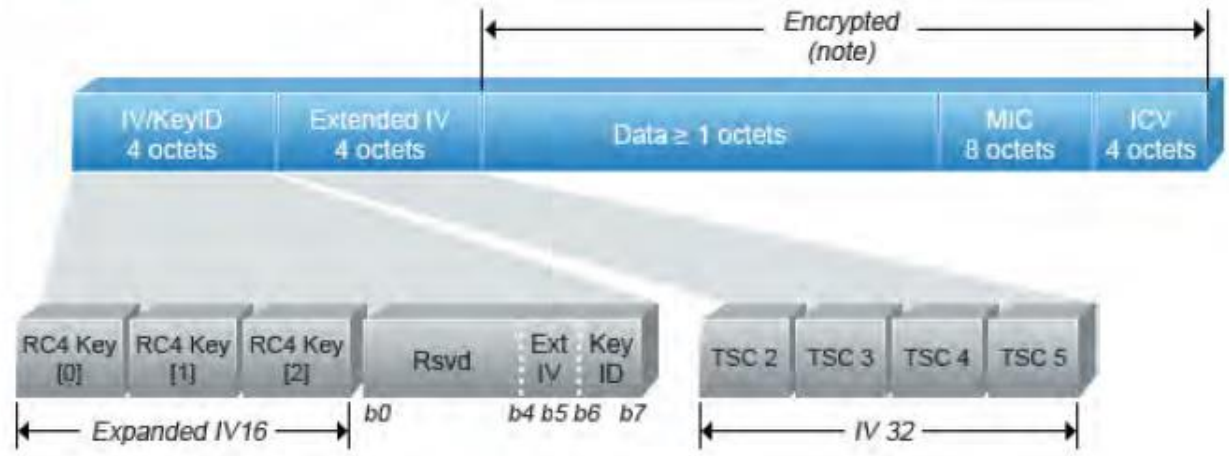
Описание сигнала тревоги и возможные причины

Новейший стандарт IEEE 802.11i включает в себя TKIP (Протокол ограничения по времени целостности ключа) и MIC (Контрольная сумма целостности сообщения) в качестве рекомендуемых протоколов конфиденциальности данных. Wi-Fi Alliance также рекомендует протоколы TKIP и MIC в своей спецификации WPA (Защищенный беспроводной доступ). Трафик WLAN, зашифрованный с помощью протоколов TKIP и MIC, защищает от подделки пакетов и атак путем повтора перехваченных данных. Что наиболее важно, протокол TKIP невосприимчив к уязвимости, создаваемой статическим ключом WEP, и атакам, возникающим в результате повторного использования ключа. Наряду с MIC, протокол TKIP также обеспечивает микширование ключей для каждого пакета, что помогает предотвратить многие атаки потоком ключей.



Temporal Key	Временный ключ
Phase 1 Key mixing	Этап 1 Микширование ключей
TTAK Key	Ключ TTAK
Phase 2 Key mixing	Этап 2 Микширование ключей
WEP seed(s)…	Сид(ы) WEP (представлен как WEP IV + ключ RC4)
MIC Key	Ключ MIC
SA+DA+priority…	SA+DA+ приоритет Открытый текст MSDU Данные
Plaintext MSDU+MIC	Открытый текст MSDU+MIC
Fragment(s)	Фрагмент(ы)
Plaintext MPDU	Открытый текст MPDU
WEP Encapsulation	Инкапсуляция WEP
Ciphertext MPDU(s)	Зашифрованный текст MPDU

Алгоритм шифрования TKIP и MIC устраняет слабые места статического WEP, а также предотвращает подделку пакетов и атаку путем повтора перехваченных данных.



Encrypted (note)	Зашифрованная часть
IV/KeyID 4 octets	IV/KeyID 4 октета
Extended IV 4 octets	Увеличенный IV 4 октета
Data ≥ 1 octet	Данные ≥ 1 октет
MIC 8 octets	MIC 8 октетов
ICV 4 octets	ICV 4 октета
Key	Ключ
Expanded IV 16	Расширенный IV 16

Кадры с шифрованием TKIP и MIC расширяют исходные данные на 20 байтов для более надежного шифрования и проверки целостности

В отличие от базирующегося на AES шифрования CCMP, протокол TKIP обычно не требует обновления оборудования. Многие производители оборудования WLAN (включая Cisco) добавили поддержку протоколов TKIP и MIC в свои последние прошивки и драйверы.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает трафик WLAN, не защищенный шифрованием TKIP, и подает сигнал тревоги. Приложение AirMagnet WiFi Analyzer рекомендует обновить эти устройства до последней версии прошивки и перенастроить их для включения шифрования TKIP.

Access Point Down (Точка доступа не работает)

Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer контролирует радиочастотное излучение всех точек доступа для поддержания работоспособности сети WLAN. Беспроводные услуги часто прерывается из-за отказов точек доступа, связанных, например, со сбоем питания, повреждением антенны, блокировкой радиопередачи и т.п. Этот сигнал тревоги появляется всякий раз, когда точка доступа выходит из строя по любой причине.

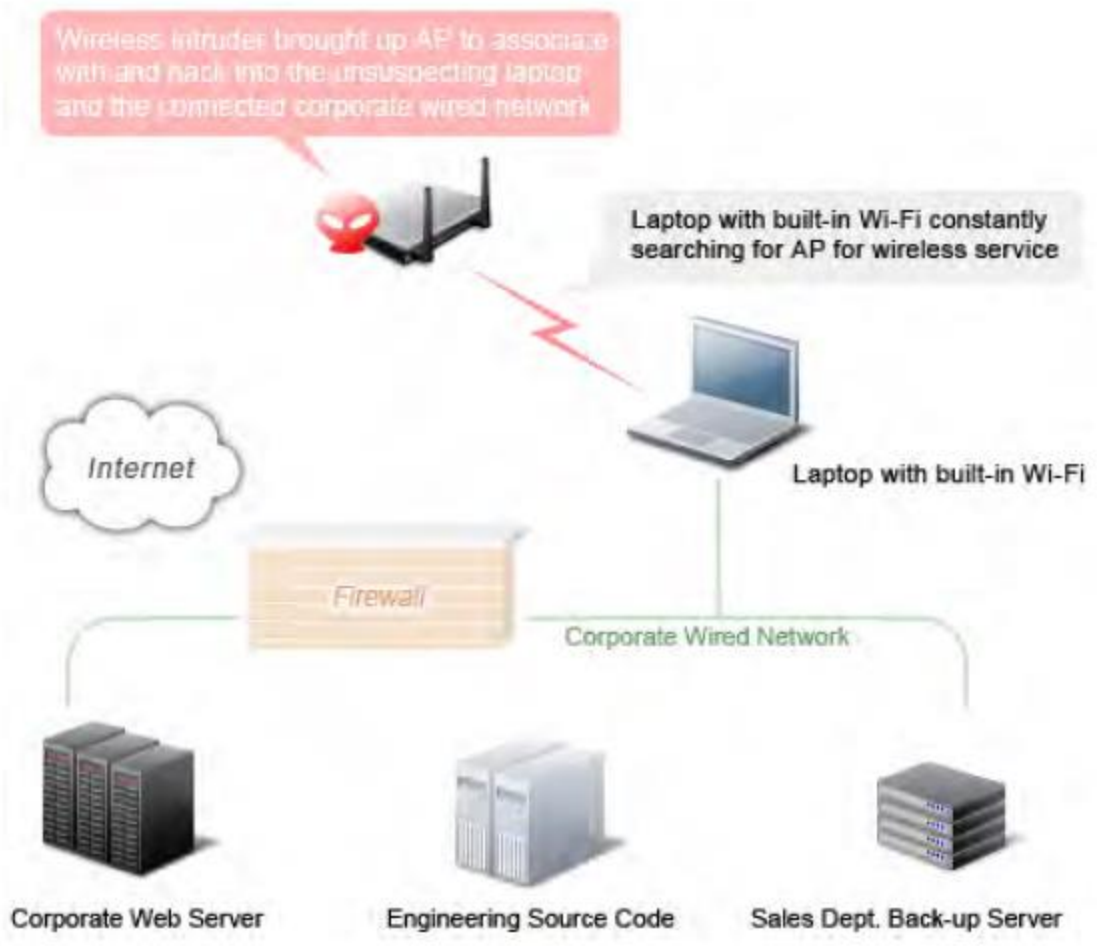
Решение AirMagnet

Если приложение AirMagnet WiFi Analyzer получает список точек доступа, который является тем же списком, что используется для обнаружения мошеннических точек доступа, то может подавать сигналы тревоги, когда любая из включенных в список точек доступа не слышна ни одному из датчиков AirMagnet SmartEdge. Этот сигнал тревоги имеет первостепенное значение для способности администратора беспроводной сети обеспечить непрерывное покрытие клиентов беспроводной сети предприятия.

Exposed Wireless Station Detected (Обнаружена открытая беспроводная станция)

Описание сигнала тревоги и возможные причины

Популярность сетей WLAN приводит к тому, что в различных средах, таких как корпоративный офис, дом или публичная точка беспроводного доступа, могут использоваться пользовательские ноутбуки с несколькими профилями конфигурации WLAN. Как правило, все эти различные профили конфигурации имеют разные уровни безопасности. Например, корпоративный офис может использовать самую надежную аутентификацию и шифрование, в то время как домашняя конфигурация или конфигурация публичной точки доступа могут практически не использовать аутентификацию или шифрование. Выбор между этими профилями конфигурации с различными настройками безопасности может быть автоматическим или ручным в зависимости от реализации производителя. Если злоумышленник узнает настройки профиля, пока клиент ищет услугу, это может создать потенциальную уязвимость для системы безопасности. Изучив профили пользователей, злоумышленник может создать точку доступа, предоставляющую желаемую услугу (SSID), чтобы заманить клиента для подключения. Как только ничего не подозревающая пользовательская станция подключится к такой точке доступа, злоумышленник получит к ней доступ по сети.



Wireless intruder brought up…	Злоумышленник организует подставную точку доступа для подключения пользователя и проникает в его ноутбук и корпоративную проводную сеть, к которой он подключен.
Laptop with build-in…	Ноутбук с встроенным адаптером Wi-Fi постоянно находится в поиске точки доступа для получения беспроводных услуг.
Internet	Интернет
Laptop with build-in Wi-Fi	Ноутбук с встроенным адаптером Wi-Fi
Firewall	Брандмауэр
Corporate Wired Network	Проводная корпоративная сеть
Corporate Web Server	Корпоративный веб-сервер

Engineering Source Code	Разработка исходного кода
Sales Dept. Back-up Server	Резервный сервер отдела продаж

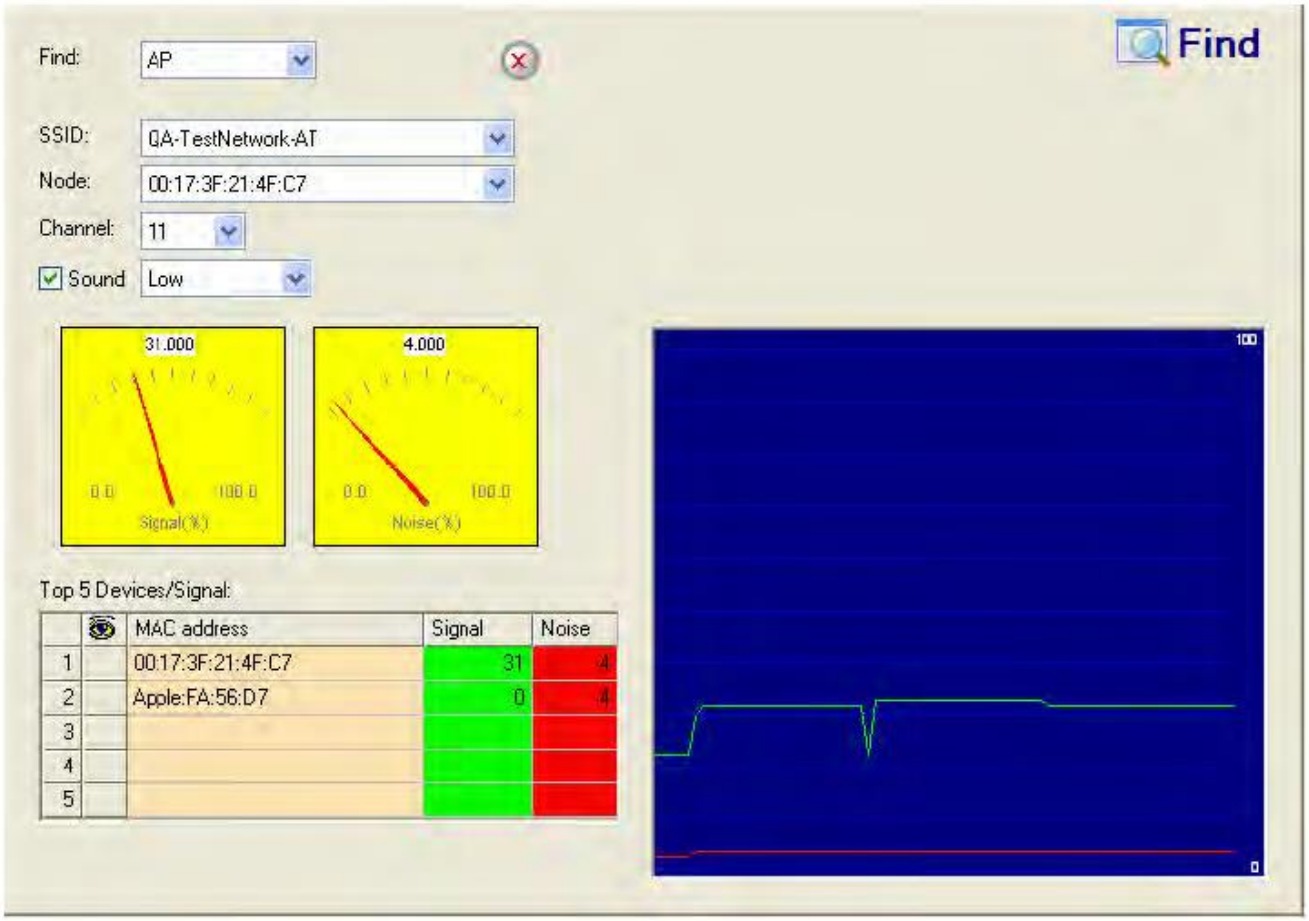
Ноутбук с открытым подключением к беспроводной локальной сети рискует раскрыть данные, хранящиеся на нем и в корпоративной проводной сети

Приложение AirMagnet WiFi Analyzer обнаруживает клиентские станции, которые постоянно ищут возможность подключения, тем самым оставляя себя уязвимыми. Как правило, это клиентские станции, неправильно настроенные вручную или автоматически с помощью переключателя выбора профиля производителя. Этот сценарий даже более опасен для предприятия, где использование беспроводной связи запрещено. Обычно такая угроза может принимать следующие формы:

- Ноутбук со встроенным адаптером Wi-Fi используется дома с минимальной защитой беспроводной сети или без нее.
- Тот же ноутбук используется на работе, где сети WLAN запрещены.
- Для обеспечения связи ноутбук подключается к проводной локальной сети предприятия.
- Встроенная в ноутбук карта Wi-Fi в течение всего дня продолжает поиск беспроводных услуг.
- Злоумышленник устанавливает точку доступа для соединения с таким ноутбуком.
- После соединения злоумышленник получает доступ к ноутбуку.
- Поскольку ноутбук также подключен к проводной локальной сети предприятия, это подвергает риску проводную сеть.

Решение AirMagnet

Станции, которые открыты и являются частью ACL (списка контроля доступа), необходимо обнаружить с помощью инструмента FIND (Найти). Администратор WLAN должен уведомить владельца или предпринять соответствующие действия в соответствии с политикой безопасности компании.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Device Unprotected by PEAP (Устройство не защищено PEAP)

Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer отслеживает транзакции 802.1x и их конкретные типы EAP (Extensible Authentication Protocol – Протокол расширенной аутентификации). Среди всех типов EAP (таких как PEAP, TLS, TTLS, LEAP, OTP и т.д.) особого внимания заслуживает PEAP (Protected EAP). Приняв PEAP в качестве метода аутентификации, вы лучше защитите свой протокол безопасности аутентификации 802.1x с помощью TLS (Transport Layer Security – безопасность транспортного уровня). Работающие в PEAP методы EAP обладают встроенными преимуществами, которые касаются:

- защиты личности
- устойчивости к атакам по словарю
- согласования защиты от атаки путем повтора перехваченных данных
- защиты заголовка
- защищенного завершения при подделке пакетов, лавинной рассылке и атаке типа «отказ в обслуживании»
- фрагментации и повторного подключения
- быстрого переподключения
- проверенного и независимого управления ключами

Многие производители оборудования WLAN (включая Cisco) недавно с обновлением прошивки добавили поддержку PEAP.

Решение AirMagnet

На эту сигнализацию приложения AirMagnet WiFi Analyzer можно положиться в деле предупреждения об устройствах, которые не используют PEAP. Убедитесь, что метод аутентификации PEAP реализован на всех устройствах в беспроводной среде.

802.11g AP with Short Slot Time (Точка доступа 802.11g с коротким интервалом ответа)

Описание сигнала тревоги и возможные причины

Использование в сети (только) 802.11g механизма короткого интервала ответа IEEE 802.11g (интервал времени 9 микросекунд) улучшает пропускную способность WLAN за счет сокращения времени ожидания передатчика гарантировано свободного канала. В соответствии с разделом 7.3.1.4 спецификации IEEE 802.11g точка доступа должна объявлять о длинном интервале ответа (20-микросекундный интервал времени) в сигнале своего маяке, когда имеется подключенная станция, например, устройство 802.11b, которая не поддерживает короткий интервал ответа. В тех случаях, когда данная спецификация не соблюдается (известно, что многие устройства 802.11g нарушают это правило), результатом будет отсутствие координации и потенциальное наложение передач, что приведет к коллизиям кадров и снижению пропускной способности.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает способность устройств WLAN поддерживать механизм коротких интервалов ответа. Как только приложение обнаруживает, что точка доступа объявляет о работе с короткими интервалами ответа, несмотря на наличие устройств, не способных их поддерживать, подается сигнал тревоги о производительности 802.11g для предупреждения администратора сети о возможном ухудшении характеристик.

802.11g AP Beacons Wrong Protection (Неверная защита сигналов маяка точки доступа 802.11g)

Описание сигнала тревоги и возможные причины

В смешанной среде WLAN 802.11b и 802.11g стандарт IEEE 802.11g задает механизмы защиты, позволяющие устройствам 802.11g и 802.11b не мешать друг другу. Поскольку устройство 802.11b (использующее модуляцию CCK) не способно обнаружить сигнал 802.11g (где используется модуляция OFDM) в том же рабочем диапазоне 2,4 ГГц, устройство 802.11b может осуществлять передачу поверх передачи 802.11g OFDM, вызывая коллизии пакетов. Для решения этой проблемы стандарт IEEE 802.11g определяет два механизма защиты: RTS/CTS и CTS-to-self. Управление осуществляется точкой доступа 802.11g, которая объявляет и запускает использование механизма защиты. Поскольку использование механизма защиты может снизить производительность сети, стандарт IEEE 802.11g не требует обязательного использования механизмов защиты в смешанной среде .11b и .11g. Однако это очень важное решение при развертывании сети 802.11g. Говоря коротко, отключение механизма защиты полезно только при очень небольшом объеме трафика 802.11b.

В той среде, где защита действительно необходима, неисправные или неправильно настроенные точки доступа, не объявляющие механизмы защиты, могут значительно снизить производительность. Было замечено, что многие точки доступа стандарта до 802.11g не реализуют механизм защиты (и даже многие из тех, что реализуют, делают это неправильно). Даже если реализация производителя верна, пользователь все равно может неправильно настроить механизм защиты, отключив его, когда это необходимо.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer наблюдает и отслеживает статус сосуществования 802.11b и 802.11g в канале. Когда механизм защиты отключается точкой доступа для развертывания смешанного режима b/g, подается сигнал тревоги, требующий дальнейшего расследования. Для профилирования трафика 802.11g и 802.11b и выбора конфигурации механизма защиты можно использовать экран Channel (Канал) приложения AirMagnet Wi-Fi Analyzer.

802.11g Protection Mechanism not Implemented (Механизм защиты 802.11g не реализован)

Описание сигнала тревоги и возможные причины

В смешанной среде WLAN 802.11b и 802.11g стандарт IEEE 802.11g задает механизмы защиты, позволяющие устройствам 802.11g и 802.11b не мешать друг другу. Поскольку устройство 802.11b (использующее модуляцию CCK) не способно обнаружить сигнал 802.11g (где используется модуляция OFDM) в том же рабочем диапазоне 2,4 ГГц, устройство 802.11b может осуществлять передачу поверх передачи 802.11g OFDM, вызывая коллизии пакетов. Для решения этой проблемы стандарт IEEE 802.11g определяет два механизма защиты: RTS/CTS и CTS-to-self. Управление осуществляется точкой доступа 802.11g, которая объявляет и запускает использование механизма защиты. Клиентские станции 802.11g должны следить за объявлением точки доступа об использовании механизма защиты.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает поведение клиентов 802.11g в отношении использования механизма защиты. Если они нарушают рекомендации своей точки доступа, не используя механизм защиты в смешанной среде WLAN 802.11b и 802.11g, AirMagnet подает этот сигнал тревоги, чтобы предупредить администратора WLAN о необходимости внесения исправлений. Воздействие такого нарушения может заключаться в отсутствии координации и потенциальном перекрывании передач от устройств 802.11b, что приводит к коллизии кадров WLAN (.11b и .11g) и снижению пропускной способности. Типовые причины этого нарушения следующие:

- Оборудование стандарта до 802.11g, не поддерживающее механизм защиты
- Ошибка пользователя в настройке конфигурации

802.11g Pre-Standard Device (Устройство предварительного стандарта 802.11g)

Описание сигнала тревоги и возможные причины

Пока готовился стандарт IEEE 802.11g, несколько производителей выпускали продукты по предварительному стандарту 802.11g, что нарушало стандарт, ратифицированный позже. Устройствами предварительного стандарта не были реализованы некоторые очень важные функции 802.11g, доработанные на поздней стадии. Эти важные функции включают, среди прочего, механизм защиты 802.11b и короткий интервал ответа.

Решение AirMagnet

Помимо наблюдения за этими конкретными нарушениями функций стандарта 802.11g, приложение AirMagnet WiFi Analyzer обнаруживает использование протокола предварительного стандарта 802.11g (черновой вариант 802.11g), чтобы идентифицировать соответствующие устройства. Как только эти устройства будут обнаружены, приложение AirMagnet Wi-Fi Analyzer порекомендует проконсультироваться у производителя оборудования, как получить последнее обновление прошивки точки доступа, чтобы она была полностью совместима с 802.11g и, что наиболее важно, чтобы ваши устройства стандартов 802.11b и 802.11g не мешали друг другу.

802.11g Device Using Non-Standard Data Rate (Устройство 802.11g использует нестандартную скорость передачи данных)

Описание сигнала тревоги и возможные причины

Стандарт 802.11g поддерживает скорость передачи данных до 54 Мбит/с; однако во избежание коллизий из-за межкадрового интервала и механизма отката с возвратом по случайному закону на практике пропускная способность намного ниже 54 Мбит/с. Различные поставщики чипсетов предлагают запатентованные технологии, позволяющие увеличить теоретическую скорость передачи данных до 108 Мбит/с. Реализации такой высокоскоростной передачи включают Super G, Turbo mode, Packet Burst и др.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer способно обнаружить использование нестандартных настроек скорости, даже если ваша текущая карта WLAN не поддерживает такие скорости. Если вы хотите включить подобные проприетарные реализации в свою сеть WLAN, следует обратить внимание на следующее:

- Некоторые высокоскоростные реализации используют технологии объединения каналов, которые расширяют использование радиочастотного спектра за пределы исходного канала 802.11g (22 МГц на канал). Если использовать эту функцию, возможно, придется пересмотреть распределение каналов, полученное при первоначальном обследовании площадки.
- Для достижения нестандартной высокой скорости передачи точки доступа и клиенты должны быть созданы одним и тем же производителем устройств или чипсетов. В сетях, где используются клиентские устройства разных производителей, высокая скорость передачи и пропускная способность могут быть ненадежными.

802.11g Protection Mechanism Overhead (Служебные данные механизма защиты 802.11g)

Описание сигнала тревоги и возможные причины

В смешанной среде WLAN 802.11b и 802.11g стандарт IEEE 802.11g задает механизмы защиты, позволяющие устройствам 802.11g и 802.11b не мешать друг другу. Поскольку устройство 802.11b (использующее модуляцию CCK) не способно обнаружить сигнал 802.11g (где используется модуляция OFDM) в том же рабочем диапазоне 2,4 ГГц, устройство 802.11b может осуществлять передачу поверх передачи 802.11g OFDM, вызывая коллизии пакетов. Для решения этой проблемы стандарт IEEE 802.11g определяет два механизма защиты: RTS/CTS и CTS-to-self. Управление осуществляется точкой доступа 802.11g, которая объявляет и запускает использование механизма защиты. Поскольку использование механизма защиты может снизить производительность сети, стандарт IEEE 802.11g не требует обязательного использования механизмов защиты в смешанной среде .11b и .11g. Однако это очень

важное решение при развертывании сети 802.11g. Говоря коротко, отключение механизма защиты полезно только при очень небольшом объеме трафика 802.11b.

В идеале развертывание WLAN с использованием стандарта 802.11g намного эффективнее при использовании только устройств 802.11g. В этом случае механизм защиты для работы в смешанном режиме не требуется и, следовательно, не добавляет никаких дополнительных служебных данных на обеспечение защиты.

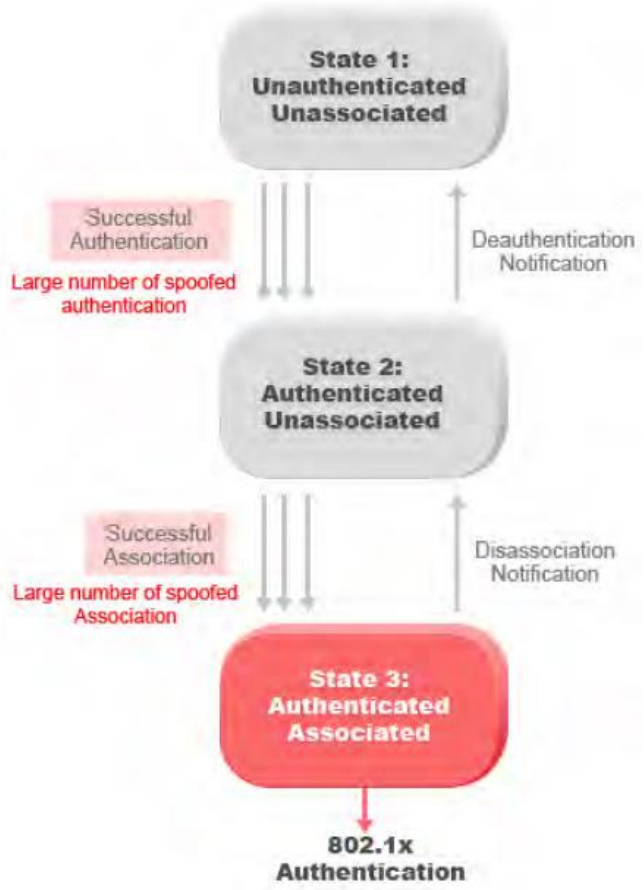
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer отслеживает использование только одного стандарта и механизма защиты. Когда служебные данные защиты повторно появляются в среде, ранее содержавшей только устройства 802.11g, приложение AirMagnet WiFi Analyzer выдает сигнал тревоги для проверки чистоты среды.

Denial-of-Service Attack: Unauthenticated Association (Атака типа «отказ в обслуживании»: Подключение без аутентификации)

Описание сигнала тревоги и возможные причины

Эта форма атаки типа «отказ в обслуживании» пытается исчерпать ресурсы точки доступа, в частности, таблицу подключения клиентов, путем заполнения точки доступа большим количеством подключений эмулированных и поддельных клиентов. На уровне 802.11 аутентификация с совместно используемым ключом (Shared-key) является ошибочной и теперь редко используется. Единственной альтернативой является открытая аутентификация (Open) (нулевая аутентификация), основанная на проверке подлинности более высокого уровня, такой как 802.1x или VPN. Открытая аутентификация позволяет любому клиенту аутентифицироваться, а затем подключиться. Для заполнения таблицы подключения клиентов целевой точки доступа злоумышленник, использующий подобную уязвимость, может эмулировать большое количество клиентов, создав множество клиентов, достигающих состояния 3, как показано на рисунке ниже. После переполнения таблицы подключений клиентов легитимные клиенты не смогут подключаться, что приведет к отказу в обслуживании.



State 1: …	Состояние 1: Аутентификация не пройдена, нет соединения
Successful Authentication	Успешная аутентификация
Deauthentication Notification	Извещение о деаутентификации
Large number of spoofed authentication	Большое количество поддельных аутентификаций
State 2:…	Состояние 2: Аутентификация пройдена, нет соединения
Successful Association	Успешное подключение
Diassociation Notification	Извещение о разъединении
Large number of spoofed Association	Большое количество поддельных подключений
State 3:…	Состояние 3: Аутентификация пройдена, соединение установлено
802.1x Authentication	Аутентификация 802.1x

Большое количество подключений эмулированных клиентов переполняет таблицу подключения клиентов на точке доступа

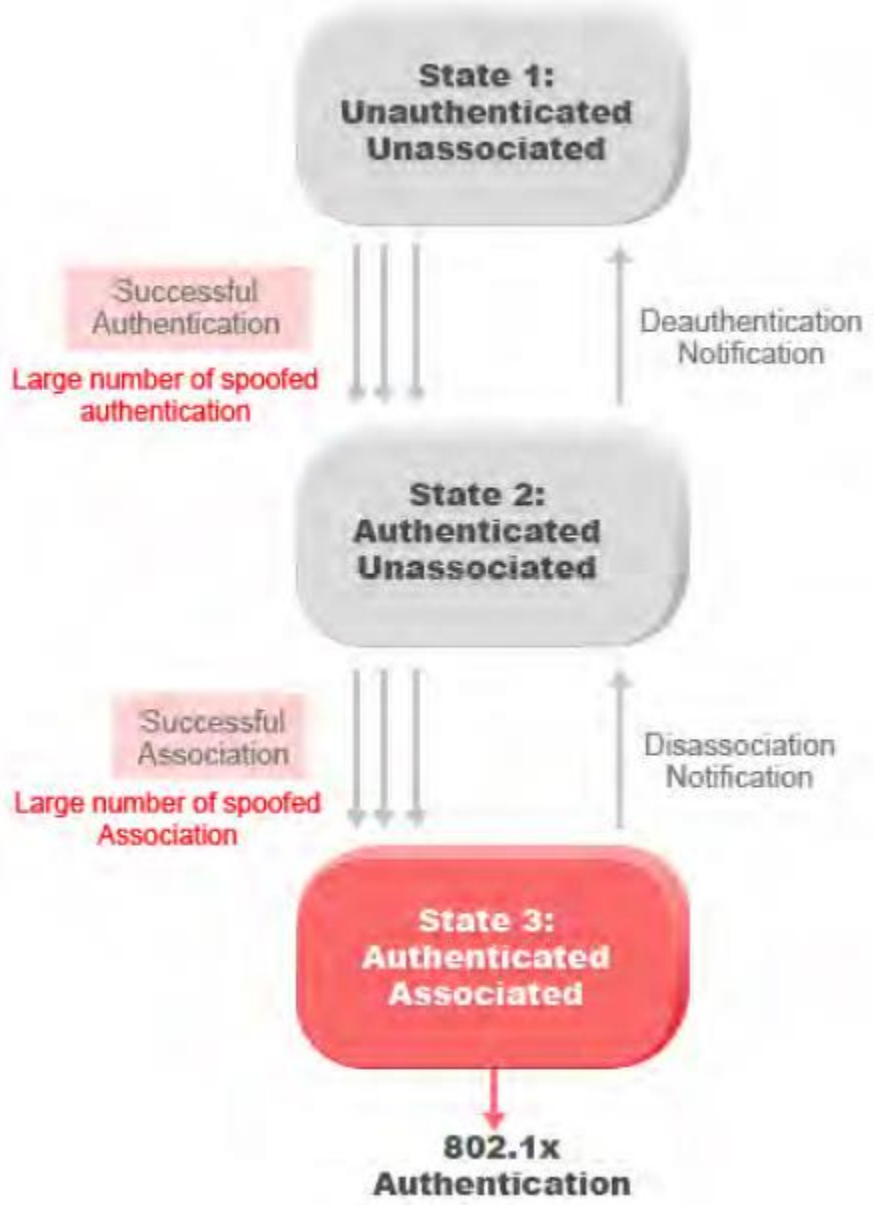
Решение AirMagnet

Чтобы обнаружить эту форму DoS-атаки, приложение AirMagnet WiFi Analyzer обнаруживает поддельные MAC-адреса и отслеживает последующие действия 802.1x и обмен данными после успешного установления связи с клиентом. Если приложение AirMagnet Wi-Fi Analyzer сообщает об этой атаке, можно использовать активные инструменты AirMagnet (проведения обследования, измерения производительности, DHCP), чтобы проверить, правильно ли работает точка доступа. Также можно войти в эту точку доступа, чтобы проверить ее таблицу подключений на количество подключенных клиентов.

Denial-of-Service Attack: Association Flood (Атака типа «отказ в обслуживании»: Флуд подключений)

Описание сигнала тревоги и возможные причины

Одной из форм атаки типа «отказ в обслуживании» является попытка исчерпать ресурсы точки доступа, в частности, таблицу подключения клиентов, путем заполнения точки доступа большим количеством подключений эмулированных и поддельных клиентов. На уровне 802.11 аутентификация с совместно используемым ключом (Shared-key) является ошибочной и теперь редко используется. Единственной альтернативой является открытая аутентификация (Open) (нулевая аутентификация), основанная на проверке подлинности более высокого уровня, такой как 802.1x или VPN. Открытая аутентификация позволяет любому клиенту аутентифицироваться, а затем подключиться. Для заполнения таблицы подключения клиентов целевой точки доступа злоумышленник, использующий подобную уязвимость, может эмулировать большое количество клиентов, создав множество клиентов, достигающих состояния 3, как показано на рисунке ниже. После переполнения таблицы подключений клиентов легитимные клиенты не смогут подключаться, что приведет к отказу в обслуживании.



State 1: …	Состояние 1: Аутентификация не пройдена, нет соединения
Successful Authentication	Успешная аутентификация
Large number of spoofed authentication	Большое количество поддельных аутентификаций
Deauthentication Notification	Извещение о деаутентификации
State 2:…	Состояние 2: Аутентификация пройдена, нет соединения
Successful Association	Успешное подключение
Large number of spoofed Association	Большое количество поддельных подключений
Diassociation Notification	Извещение о разъединении
State 3:…	Состояние 3: Аутентификация пройдена, соединение установлено
802.1x Authentication	Аутентификация 802.1x

Большое количество подключений эмулированных клиентов переполняет таблицу подключения клиентов на точке доступа

Решение AirMagnet

Чтобы обнаружить эту форму DoS-атаки, приложение AirMagnet WiFi Analyzer обнаруживает поддельные MAC-адреса и отслеживает последующие действия 802.1x и обмен данными после успешного установления связи с клиентом. Если приложение AirMagnet Wi-Fi Analyzer сообщает об этой атаке, можно использовать активные инструменты AirMagnet (проведения обследования, измерения производительности, DHCP), чтобы проверить, правильно ли работает точка доступа. Также можно войти в эту точку доступа, чтобы проверить ее таблицу подключений на количество подключенных клиентов.

Rogue AP by IEEE ID (OUI) (Неавторизованная точка доступа по идентификатору IEEE (OUI))

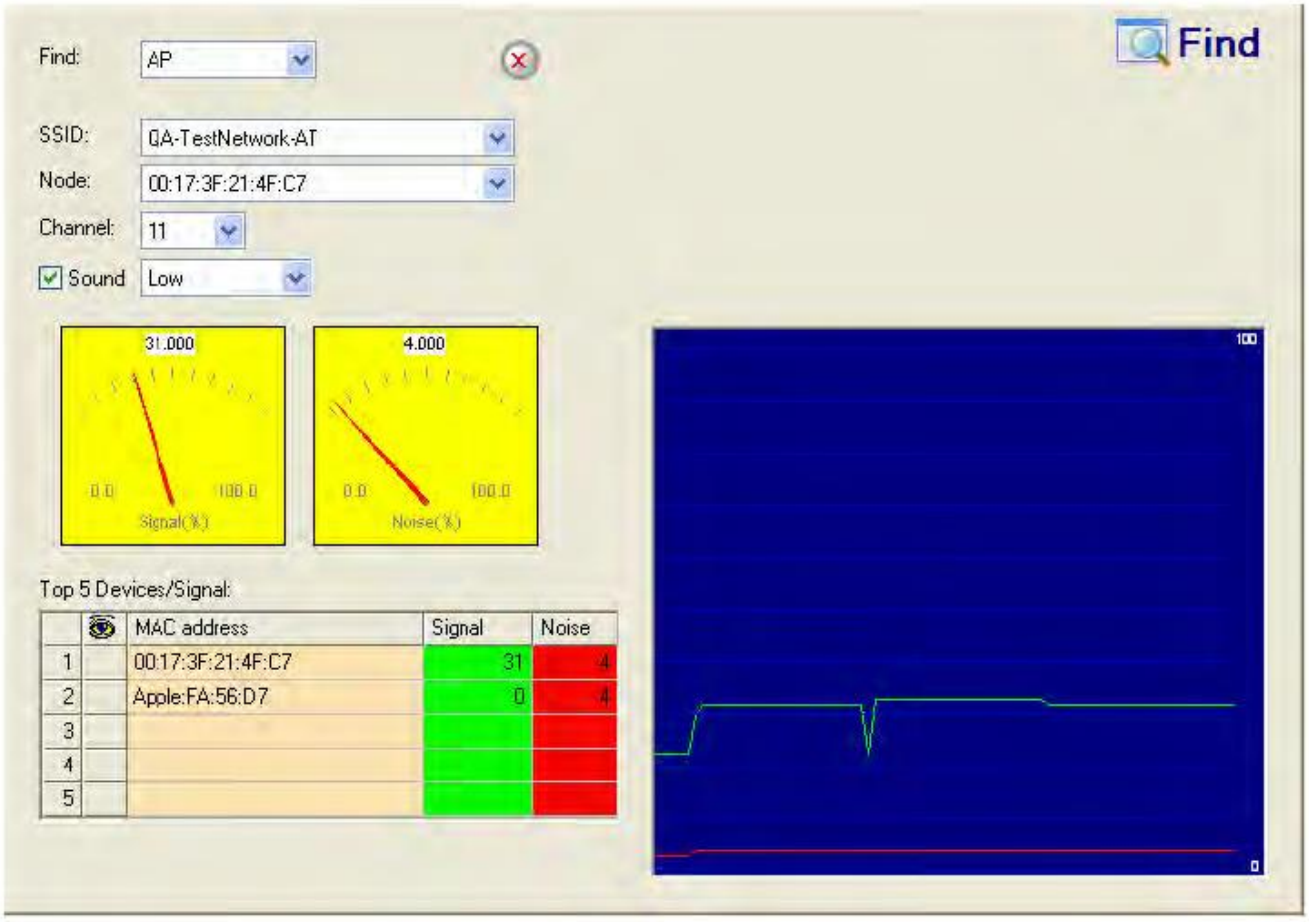
Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer предупреждает администратора WLAN о неавторизованной точке доступа, сверяясь с предварительно настроенным списком авторизованных производителей оборудования. Например, если на вашем предприятии развернуты только точки доступа Cisco Aironet или Symbol Technologies, необходимо включить Cisco и Symbol в список авторизованных производителей. После импортирования списка производителей приложение AirMagnet Wi-Fi Analyzer выдает сигнал тревоги о неавторизованной точке доступа всякий раз, когда обнаруживает точку доступа, не указанную в списке, то есть точку доступа, производителем которой не является Cisco Aironet или Symbol Technologies.

Неавторизованные точки доступа, установленные неавторизованными сотрудниками, обычно не соответствуют стандартным корпоративным методам развертывания и, таким образом, могут поставить под угрозу безопасность беспроводных и проводных сетей. Мошенническая точка доступа также может указывать на то, что проводную сеть предприятия пытается взломать злоумышленник. Обнаруженные приложением AirMagnet WiFi Analyzer неавторизованные устройства необходимо тщательно исследовать.

Решение AirMagnet

После того, как приложение AirMagnet WiFi Analyzer обнаружило неавторизованную точку доступа и подало сигнал тревоги, администратор WLAN может использовать инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer для определения местоположения неавторизованного устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Rogue Station by IEEE ID (OUI) (Неавторизованная станция по идентификатору IEEE (OUI))

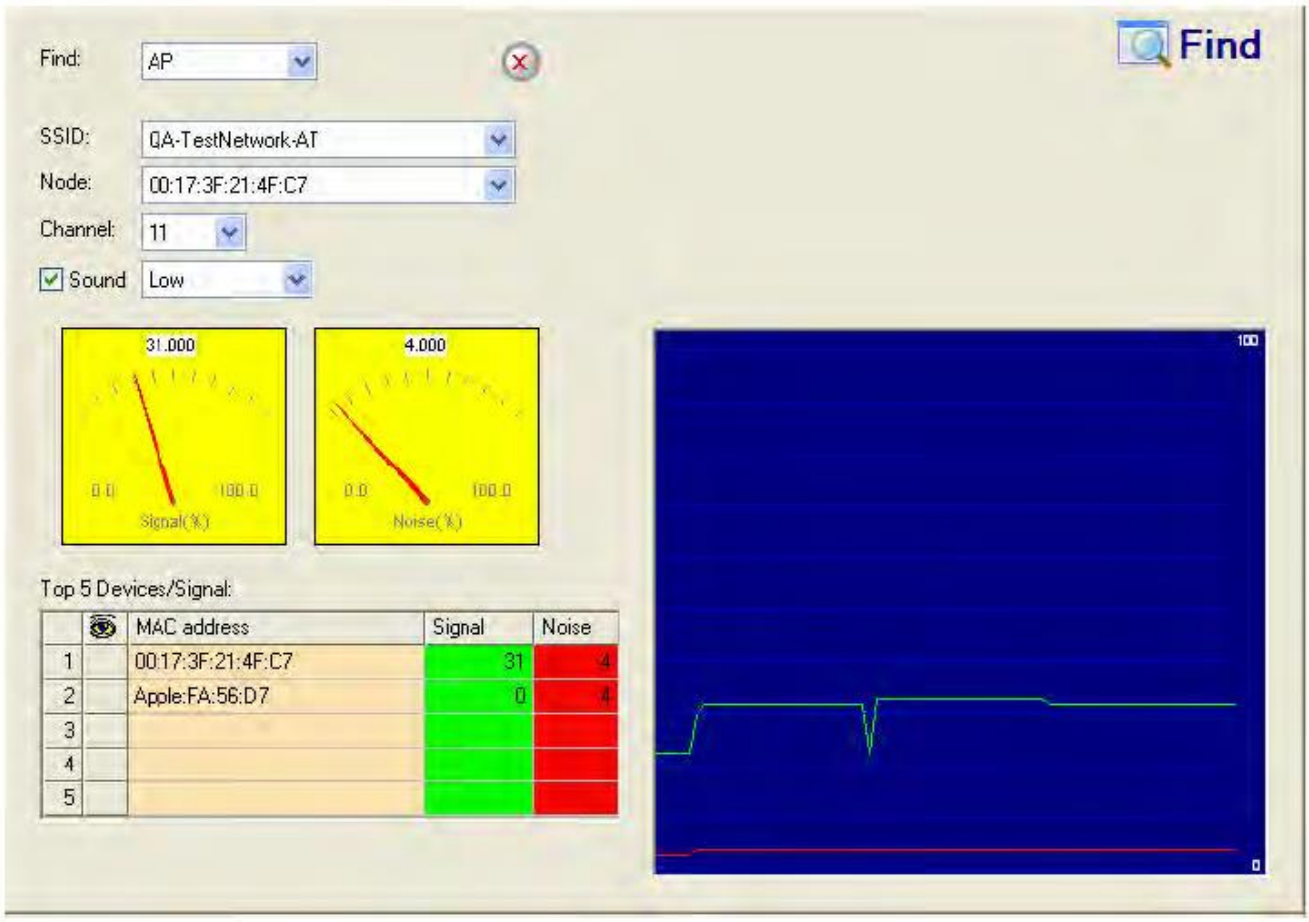
Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer предупреждает администратора WLAN о неавторизованной станции, сверяясь с предварительно настроенным списком авторизованных производителей станций. Например, если на вашем предприятии развернуты только станции Cisco Aironet или Symbol Technologies, необходимо включить Cisco и Symbol в список авторизованных производителей. После импортирования списка производителей приложение AirMagnet Wi-Fi Analyzer выдает сигнал тревоги о неавторизованной станции всякий раз, когда обнаруживает станцию, не указанную в списке, то есть станцию, производителем которой не является Cisco Aironet или Symbol Technologies.

Неавторизованные станции, установленные неавторизованными сотрудниками, обычно не соответствуют стандартным корпоративным методам развертывания и, таким образом, могут поставить под угрозу безопасность беспроводных и проводных сетей. Неавторизованная станция также может указывать на то, что проводную сеть предприятия пытается взломать злоумышленник. Обнаруженные приложением AirMagnet WiFi Analyzer неавторизованные устройства необходимо тщательно исследовать.

Решение AirMagnet

После того, как приложение AirMagnet WiFi Analyzer обнаружило неавторизованную станцию и подало сигнал тревоги, администратор WLAN может использовать инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer для определения местоположения неавторизованного устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Rogue AP by SSID (Неавторизованная точка доступа по SSID)

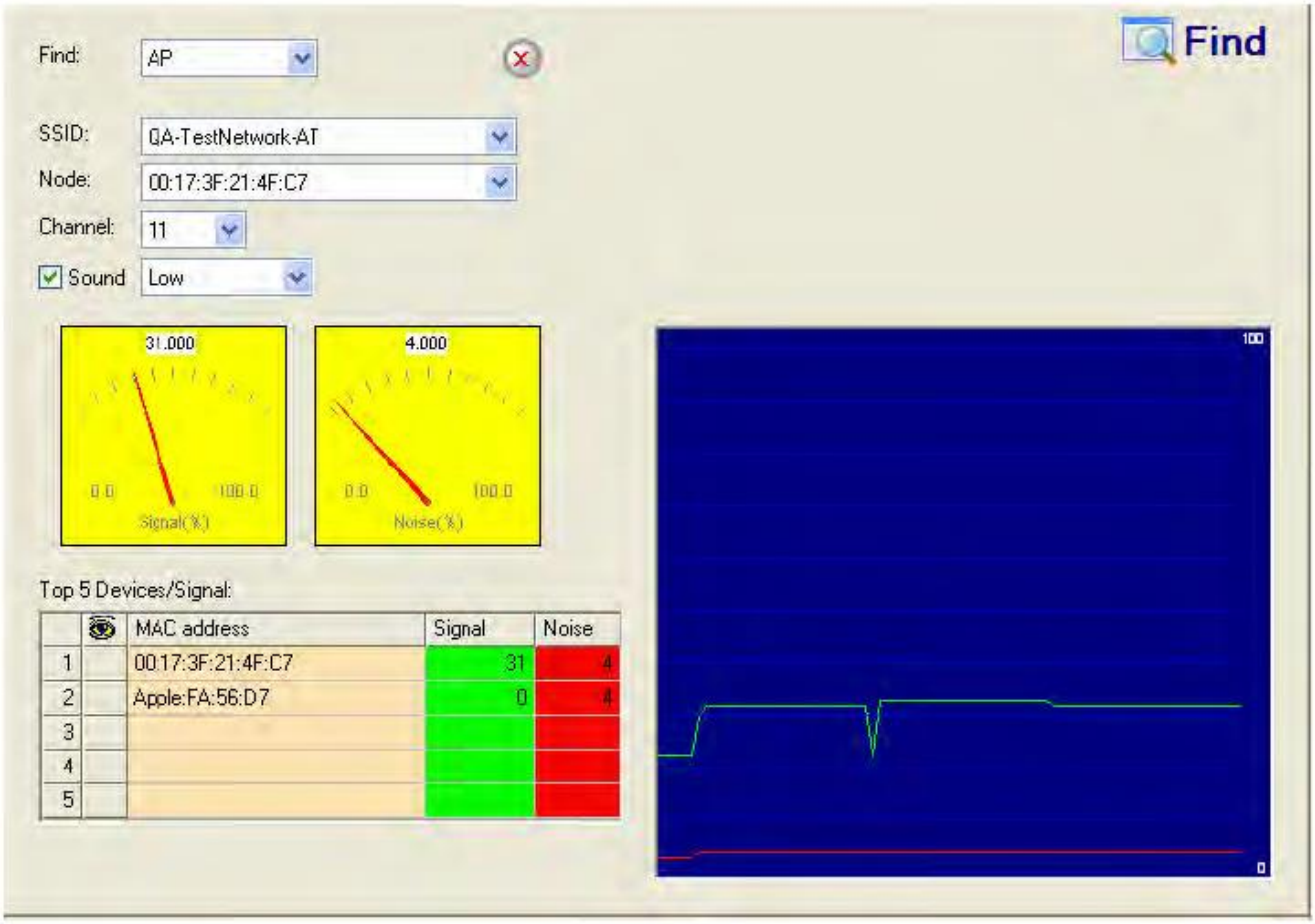
Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer предупреждает администратора WLAN о неавторизованной точке доступа, сверяясь с предварительно настроенным списком авторизованных идентификаторов SSID. Например, если ваша корпоративная WLAN настроена только с MyOfficeWlan и MyVoIPWlan, необходимо включить эти два SSID в список авторизованных идентификаторов SSID. После импортирования этого списка приложение AirMagnet WiFi Analyzer подает сигнал тревоги о неавторизованной точке доступа, когда обнаруживается точка доступа, работающая с другим идентификатором SSID.

Неавторизованные точки доступа, установленные неавторизованными сотрудниками, обычно не соответствуют стандартным корпоративным методам развертывания и, таким образом, могут поставить под угрозу безопасность беспроводных и проводных сетей. Мошенническая точка доступа также может указывать на то, что проводную сеть предприятия пытается взломать злоумышленник. Обнаруженные приложением AirMagnet WiFi Analyzer неавторизованные устройства необходимо тщательно исследовать.

Решение AirMagnet

После того, как приложение AirMagnet WiFi Analyzer обнаружило неавторизованную точку доступа и подало сигнал тревоги, администратор WLAN может использовать инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer для определения местоположения неавторизованного устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Rogue Station by SSID (Неавторизованная станция по SSID)

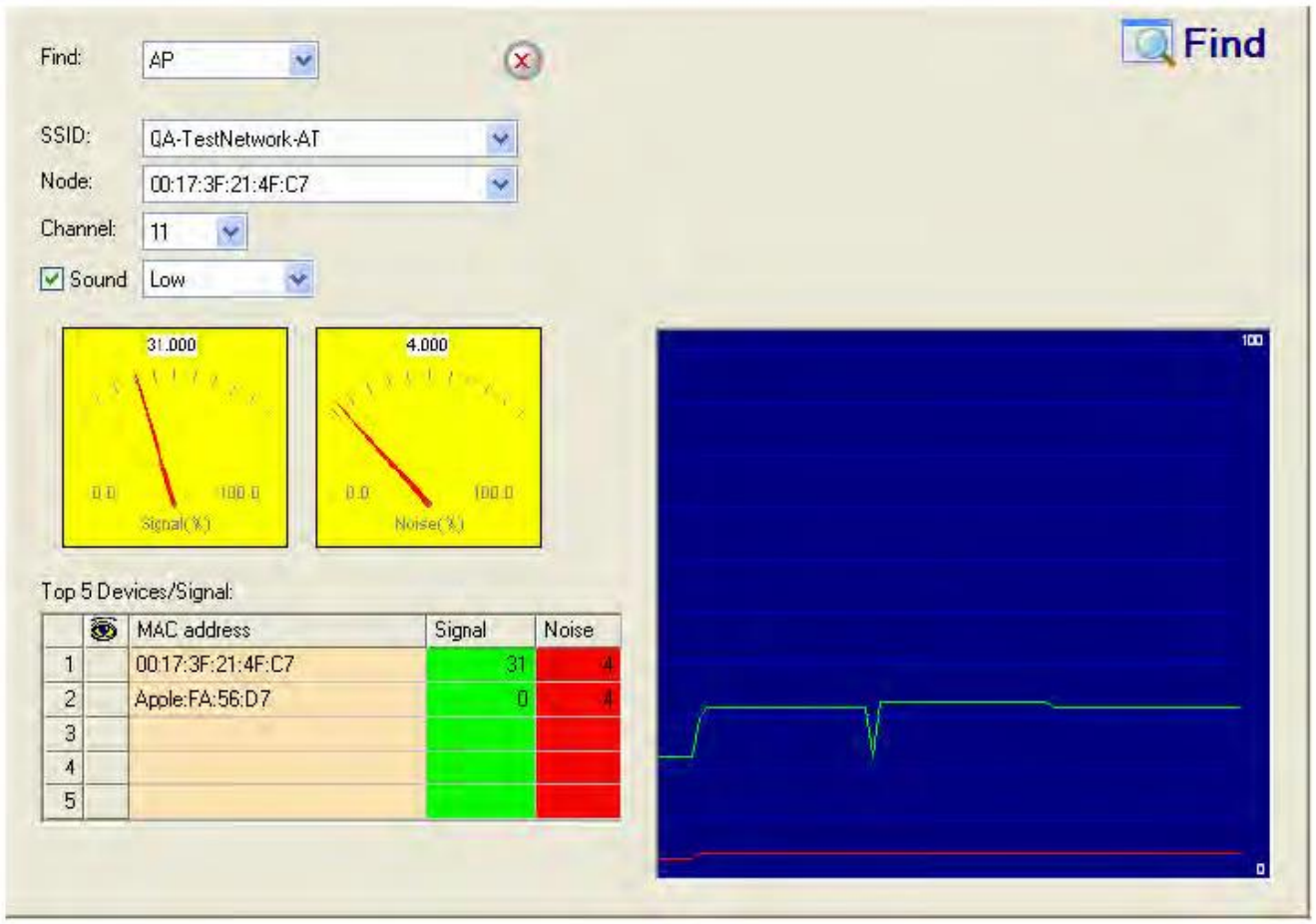
Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer предупреждает администратора WLAN о неавторизованной станции, сверяясь с предварительно настроенным списком авторизованных идентификаторов SSID. Например, если ваша корпоративная WLAN настроена только с MyOfficeWlan и MyVoIPWlan, необходимо включить эти два SSID в список авторизованных идентификаторов SSID. После импортирования этого списка приложение AirMagnet WiFi Analyzer подает сигнал тревоги о неавторизованной станции, когда обнаруживается станция, работающая с другим идентификатором SSID.

Неавторизованные станции, установленные неавторизованными сотрудниками, обычно не соответствуют стандартным корпоративным методам развертывания и, таким образом, могут поставить под угрозу безопасность беспроводных и проводных сетей. Мошенническая станция также может указывать на то, что проводную сеть предприятия пытается взломать злоумышленник. Обнаруженные приложением AirMagnet WiFi Analyzer неавторизованные устройства необходимо тщательно исследовать.

Решение AirMagnet

После того, как приложение AirMagnet WiFi Analyzer обнаружило неавторизованную станцию и подало сигнал тревоги, администратор WLAN может использовать инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer для определения местоположения неавторизованного устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Rogue AP by Wireless Media Type (Неавторизованная точка доступа по типу беспроводной среды)

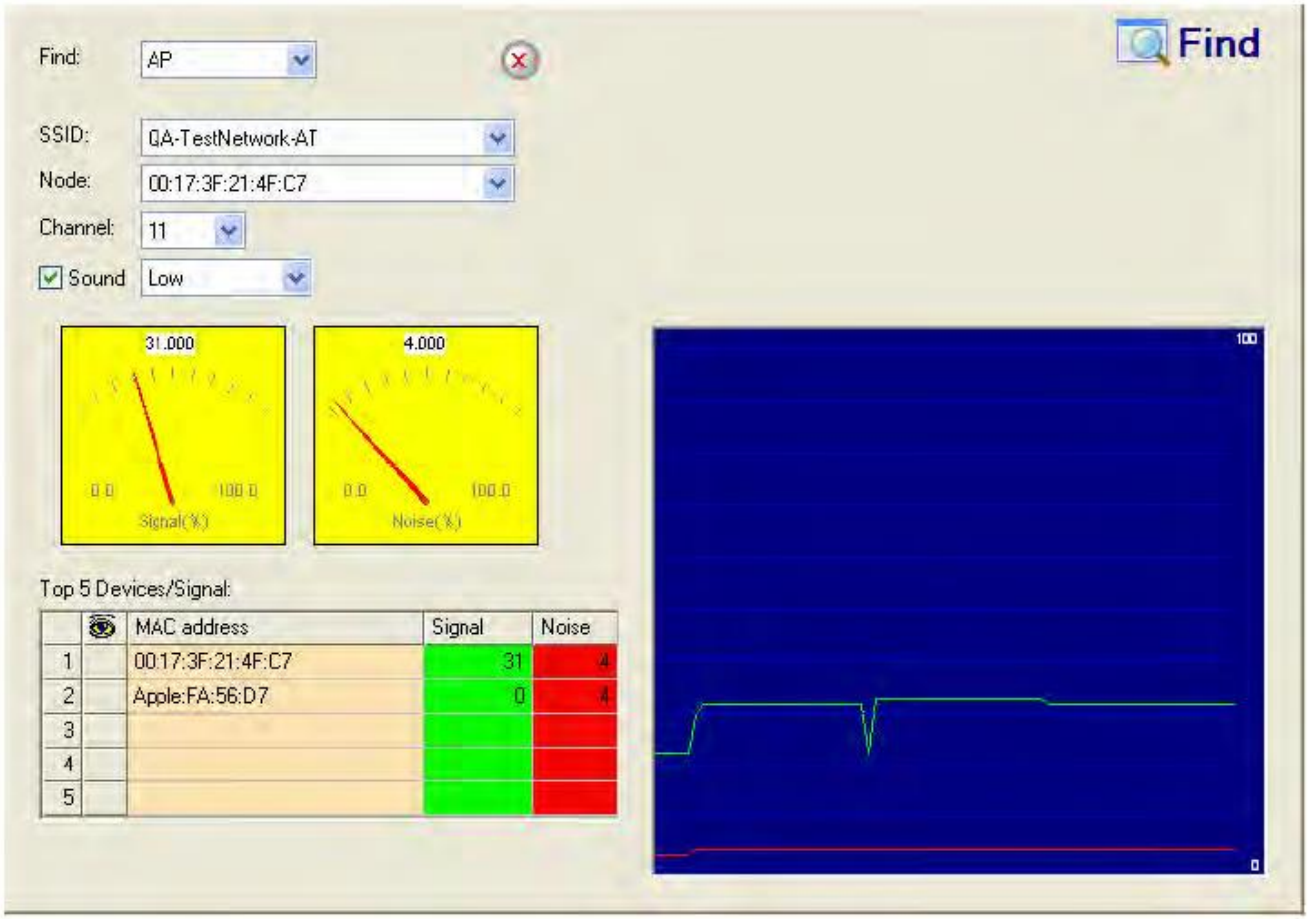
Описание сигнала тревоги и возможные причины

Приложение WiFi Analyzer предупреждает администратора WLAN о неавторизованной точке доступа, проверяя используемые предприятием стандартные рабочие радиочастоты и среду передачи данных, например, 802.11a, 802.11b, 802.11g или 802.11n. Когда приложение AirMagnet WiFi Analyzer обнаруживает точку доступа, работающую за пределами стандартной корпоративной радиочастотной среды, будет подан сигнал тревоги о мошеннической точке доступа. Например, рассмотрим случай, когда предприятие использует только точки доступа 802.11b/g/n. Если обнаружена точка доступа 802.11a, приложение AirMagnet WiFi Analyzer немедленно подаст сигнал тревоги.

Неавторизованные точки доступа, установленные неавторизованными сотрудниками, обычно не соответствуют стандартным корпоративным методам развертывания и, таким образом, могут поставить под угрозу безопасность беспроводных и проводных сетей. Мошенническая точка доступа также может указывать на то, что проводную сеть предприятия пытается взломать злоумышленник. Обнаруженные приложением AirMagnet WiFi Analyzer неавторизованные устройства необходимо тщательно исследовать.

Решение AirMagnet

После того, как приложение AirMagnet WiFi Analyzer обнаружило неавторизованную точку доступа и подало сигнал тревоги, администратор WLAN может использовать инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer для определения местоположения неавторизованного устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Rogue Station by Wireless Media Type (Неавторизованная станция по типу беспроводной среды)

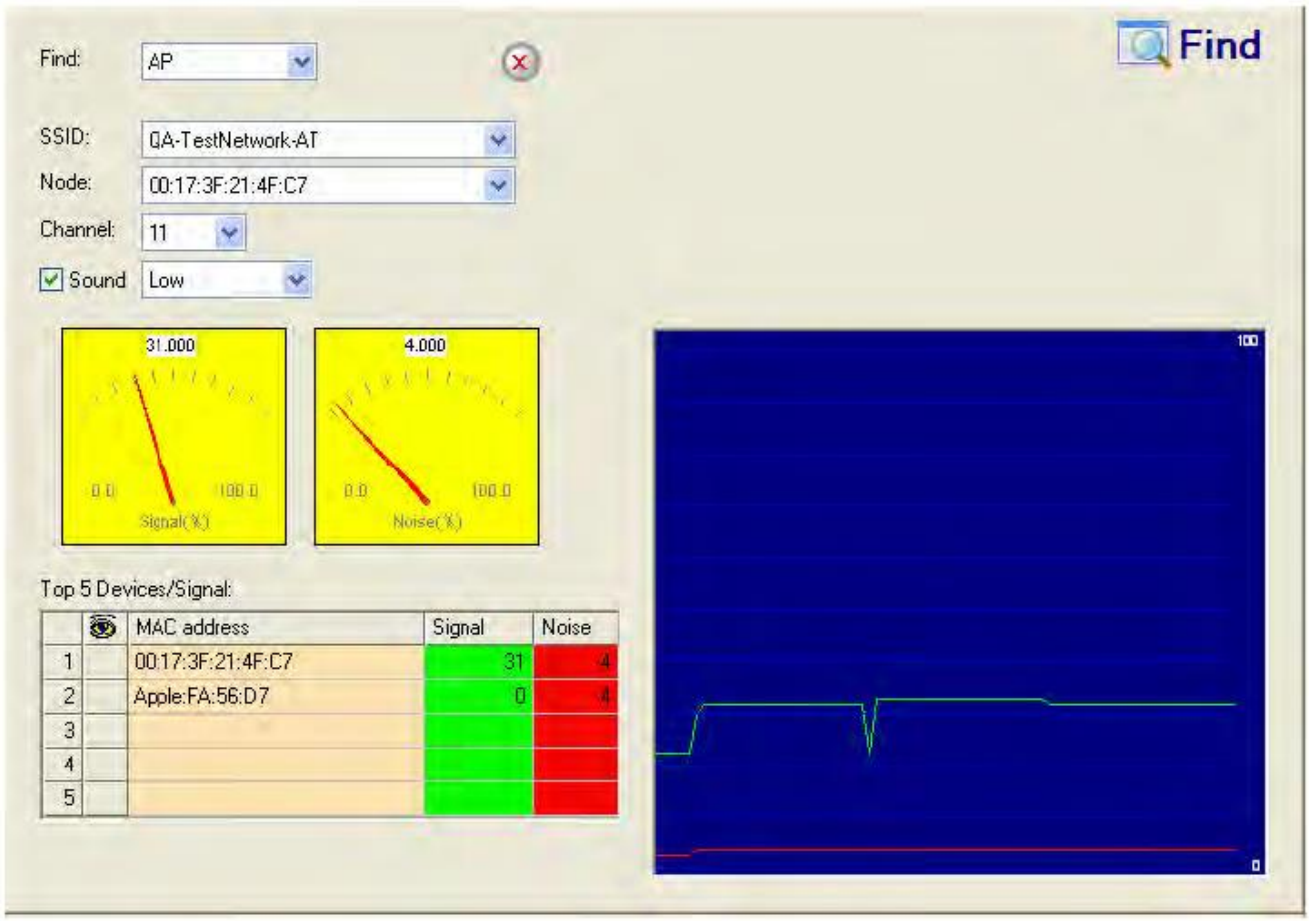
Описание сигнала тревоги и возможные причины

Приложение WiFi Analyzer предупреждает администратора WLAN о неавторизованной станции, проверяя используемые предприятием стандартные рабочие радиочастоты и среду передачи данных, например, 802.11a, 802.11b, 802.11g или 802.11n. Когда приложение AirMagnet WiFi Analyzer обнаруживает клиентскую станцию, работающую за пределами стандартной корпоративной радиочастотной среды, будет подан сигнал тревоги о мошеннической станции. Например, рассмотрим случай, когда предприятие использует только станции 802.11b/g/n. Если обнаружена станция 802.11a, приложение AirMagnet WiFi Analyzer немедленно подаст сигнал тревоги.

Неавторизованные станции, установленные неавторизованными сотрудниками, обычно не соответствуют стандартным корпоративным методам развертывания и, таким образом, могут поставить под угрозу безопасность беспроводных и проводных сетей. Мошенническая станция также может указывать на то, что проводную сеть предприятия пытается взломать злоумышленник. Обнаруженные приложением AirMagnet WiFi Analyzer неавторизованные устройства необходимо тщательно исследовать.

Решение AirMagnet

После того, как приложение AirMagnet WiFi Analyzer обнаружило неавторизованную станцию и подало сигнал тревоги, администратор WLAN может использовать инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer для определения местоположения неавторизованного устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Suspicious After-Hour Traffic Detected (Обнаружен подозрительный трафик в нерабочее время)

Описание сигнала тревоги и возможные причины

Одним из способов обнаружения попытки проникновения в систему безопасности беспроводной сети является анализ использования беспроводной сети в то время, когда не предполагается наличие какого-либо беспроводного трафика (например, в нерабочее время). Приложение AirMagnet WiFi Analyzer отслеживает шаблоны трафика в соответствии с рабочим временем, настроенным для этого сигнала тревоги, и подает предупреждения при обнаружении отклонений от нормы. К подозрительным случаям использования беспроводной сети, отслеживаемым приложением AirMagnet WiFi Analyzer в нерабочее время, относятся следующие:

- Клиентская станция инициирует запросы аутентификации или подключения к офисной сети WLAN, что может указывать на попытку нарушения безопасности.
- Беспроводной трафик данных, который может указывать на подозрительные загрузки или выгрузки по беспроводной сети.

Решение AirMagnet

При глобальном развертывании приложения AirMagnet WiFi Analyzer диапазон рабочего времени задается в соответствии с часовым поясом. Для смешанной сети WLAN офиса и производственного цеха можно задать рабочие часы (например, с 9:00 до 17:00) для SSID офисной WLAN и отдельную продолжительность рабочего периода (например, с 6:00 до 21:00) для SSID сети WLAN производственного помещения. При срабатывании этого сигнала тревоги администратор должен найти устройства, ответственные за подозрительный трафик, и предпринять соответствующие шаги для их обнаружения и удаления из беспроводной среды.

Fake APs Detected (Обнаружены фейковые точки доступа)

Описание сигнала тревоги и возможные причины

Инструмент Fake AP предназначен для защиты вашей сети WLAN. Он действует как приманка, чтобы сбить с толку злоумышленников, использующих NetStumbler, Wellenreiter, MiniStumbler, Kismet и т.п. Инструмент генерирует кадры маяка, имитируя тысячи поддельных точек доступа 802.11b. Сталкивающиеся с таким большим количеством точек доступа злоумышленники не смогут идентифицировать настоящие точки доступа, развернутые пользователем. Этот инструмент, хотя и очень эффективен в предотвращении проникновения злоумышленников, имеет множество недостатков, включая потребление полосы пропускания, ввод в заблуждение легитимных клиентских станций, вмешательство в инструменты управления WLAN и т.д. Приложение AirMagnet Wi-Fi Analyzer не рекомендует запускать инструмент Fake AP на своей сети WLAN.

Решение AirMagnet

AirMagnet рекомендует администратору найти устройство, на котором запущен инструмент Fake AP, и предпринять соответствующие шаги, чтобы удалить его из беспроводной среды.

Device Unprotected by Fortress Encryption (Устройство не защищено шифрованием Fortress)

Описание сигнала тревоги и возможные причины

Если безопасность вашей сети WLAN требует использования технологий шифрования, предоставляемых Fortress Technologies, Inc., можно включить этот сигнал тревоги, который будет предупреждать об устройствах, участвующих в обмене данными WLAN без шифрования Fortress.

Fortress Secure Gateways является накладываемым решением, поэтому его можно легко развернуть в любой сети, независимо от топологии, производителя инфраструктуры или используемой беспроводной технологии. У Fortress есть модели, подходящие для любых конкретных требований, будь то защита небольших групп пользователей WLAN или всего предприятия.

Шлюзы Fortress Secure обеспечивают безопасность между беспроводными устройствами, пользователями и сетевой инфраструктурой. Все критически важные операции безопасности - шифрование, аутентификация, проверка целостности данных, обмен ключами и сжатие данных – оптимизируются для минимизации ручного управления. Также это решение обеспечивает безопасное обслуживание нескольких точек доступа одновременно и масштабируется для различных архитектур.

Fortress Technologies предоставляет комплексное, надежное беспроводное решение, которое легко внедрить и поддерживать. Благодаря защите устройств, данных и сети, Fortress является самой надежной коммерчески доступной платформой безопасности для беспроводных сетей.

Решение AirMagnet

Необходимо включить использование шифрования Fortress для различных устройств в беспроводной среде. Данное новое предупреждение безопасности идентифицирует пользователей, которые не способны запустить Fortress Security System. Это позволит клиентам, которые заботятся о безопасности и выбрали Fortress, убедиться, что их политика аутентификации/шифрования соблюдается в каждой сети по всему миру. Комбинированное предложение продуктов объединяется в надежную инфраструктуру безопасности Fortress, которая выполняет шифрование на уровне 2, что исключает возможность для хакеров перехватывать важные сетевые данные, просматривать внутренние сетевые адреса или прерывать доступность посредством атак типа «отказ в обслуживании», а также обеспечивает безопасность AirMagnet Wi-Fi Analyzer и системы управления производительностью, которые контролируют и управляют безопасностью беспроводной сети. С помощью этого решения организации

получают в свое распоряжение все преимущества надежного беспроводного решения Fortress, которое легко внедрить и поддерживать, в сочетании с наиболее полным мониторингом мошенников, беспроводных уязвимостей и сетевых вторжений.

Device Thrashing Between 802.11g and 11b (Переключение устройства между 802.11g и 11b)

Описание сигнала тревоги и возможные причины

Стандарт IEEE 802.11g требует, чтобы устройство 802.11g было обратно совместимо со стандартом IEEE 802.11b. Для каждой передачи кадра устройство 802.11g может принимать решение по переключению между режимом 802.11b (с использованием модуляции CCK) или режимом 802.11g (с использованием модуляции OFDM). Точки доступа 802.11g используют эту функцию для поддержки смешанного режима (устройства 802.11b и 802.11g) в одной беспроводной среде. Клиентская станция 802.11g использует эту функцию для оптимизации производительности и подключения к лучшим услугам, предоставляемым точкой доступа 802.11b или 11g.

Переключение режимов является обычной функцией. Однако клиентская станция, постоянно меняющая свой радиочастотный режим между 802.11g (OFDM) и 802.11b (CCK), является свидетельством нестабильной радиочастотной среды. Это снижает пропускную способность 802.11g за счет понижения максимальной скорости передачи с 54 до 11 Мбит/с. Кроме того, это может даже вызвать прерывание обслуживания клиента, если также переключается соединение с точкой доступа. Чрезмерное переключение режимов может быть вызвано реализацией 802.11g, которая слишком чувствительна к динамическому сочетанию трафика и устройств между 802.11b и 11g. Переключение режима клиентской станции также может быть вызвано переключением режима на точках доступа.

Решение AirMagnet

Для дальнейшего изучения этой проблемы вы можете использовать страницу Infrastructure (Инфраструктура) приложения AirMagnet WiFi Analyzer и выбрать опцию просмотра List by Station (Список по станциям), чтобы отобразить историю всех сеансов, которые клиентская станция имела с различными точками доступа. Также можно контролировать переключатель радиочастотного режима клиента в реальном времени, наблюдая после выбора целевой клиентской станции на странице Infrastructure (Инфраструктура) за используемыми клиентом скоростями передачи.

AP With Flawed Power-Save Implementation (Точка доступа с некорректной реализацией энергосбережения)

Описание сигнала тревоги и возможные причины

С целью экономии энергии стандарт IEEE 802.11 задает режим энергосбережения для мобильных устройств путем их перехода в спящий режим. Пока клиент остается в спящем режиме, точка доступа буферизует предназначенные для него данные для доставки в более позднее время. Стандарт определяет квитирование режима энергосбережения, включающее следующую важную процедуру:

- Клиент сообщает точке доступа свое состояние режима энергосбережения (переходя в спящий режим).
- Точка доступа сообщает клиенту, как часто предназначенные клиенту данные будут отображаться в сигнале маяка.
- Точка доступа буферизует данные, предназначенные для находящегося в спящем режиме клиента.
- Клиент периодически просыпается, чтобы проверить сигналы маяка точки доступа и узнать, есть ли для него данные в буфере.
- Если данных нет, клиент возвращается в спящий режим. Если есть данные, клиент информирует точку доступа о своем состоянии режима энергосбережения, а точка доступа отправляет клиенту буферизованные данные.

Те точки доступа, которые не способны обеспечить данную процедуру, могут терять данные клиента. С этим связаны два хорошо известных недостатка точек доступа:

- Точка доступа не буферизует данные клиента, пока клиент находится в режиме энергосбережения.
- Точка доступа не уведомляет находящегося в режиме энергосбережения клиента о поступлении для него данных.

Оба сценария приводят к потере клиентских данных, которые в конечном итоге должны будут повторно переданы таким протоколом верхнего уровня, как TCP. Однако возникшая задержка резко снижает производительность приложения. Для некоторых приложений, например, VoIP в WLAN, потерянные данные не будут передаваться повторно, что приведет к джиттеру передачи голоса. Это может быть недопустимо, приводить к повторной передаче, длительным задержкам и снижению производительности.

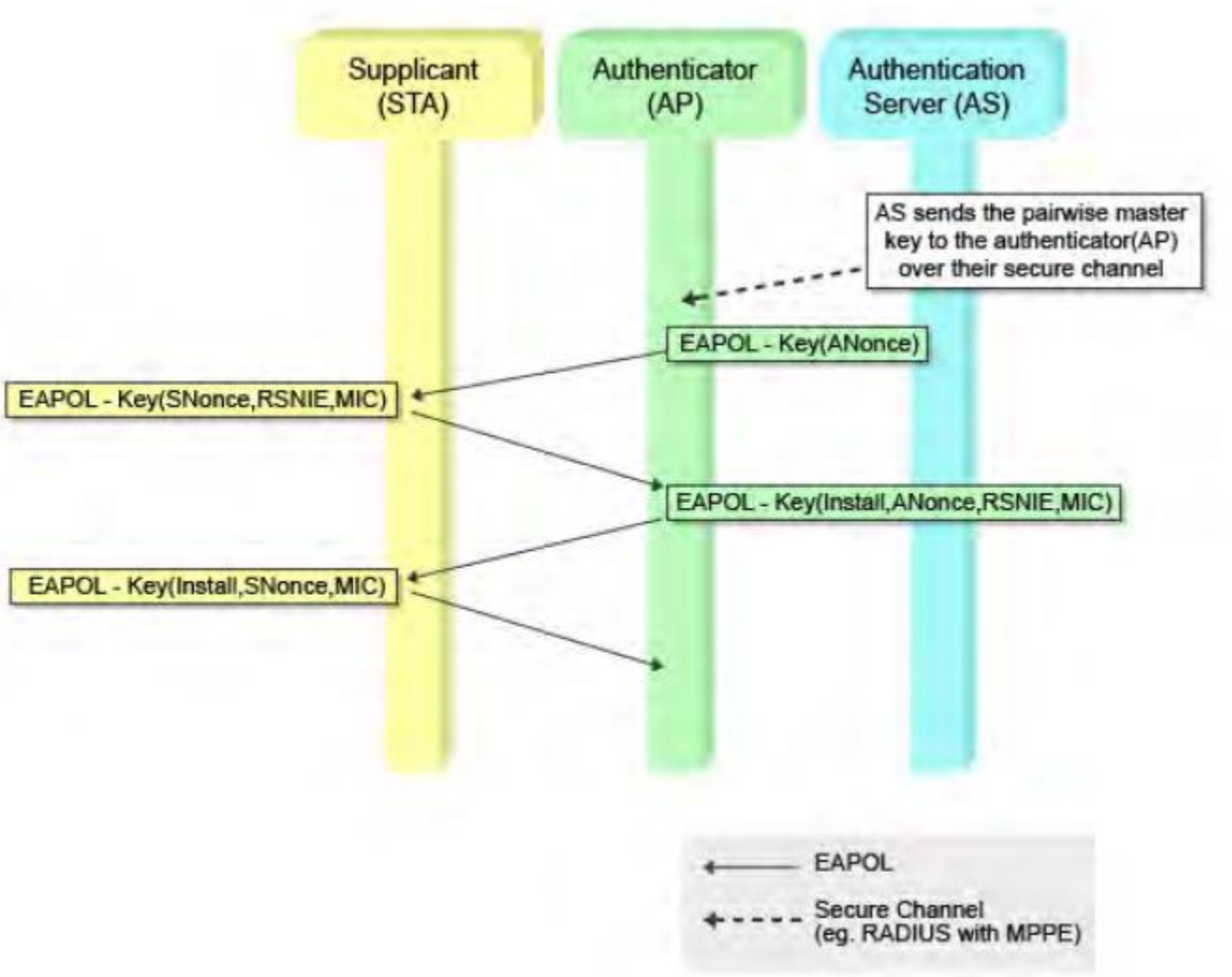
Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает точки доступа с некорректными реализациями энергосбережения 802.11, аналогичными двум упомянутым выше дефектам. Эта проблема обычно не влияет отрицательно на беспроводное подключение, но приводит к серьезному ухудшению качества обслуживания. Помочь решить эту проблему способно обновление прошивки точки доступа.

WPA or 802.11i Pre-Shared Key Used (Применяется заранее установленный совместно используемый ключ WPA или 802.11i)

Описание сигнала тревоги и возможные причины

WPA и стандарт 802.11i предоставляют механизм заранее установленного совместно используемого ключа (PSK) в качестве альтернативы использованию ключа на основе IEEE 802.1x. Для управления ключами на основе 802.1x требуется такой сервер аутентификации, как RADIUS, обеспечивающий безопасное и динамическое распределение ключей сеанса (парный главный ключ или Pairwise Master Key/PMK). Когда вместо 802.1x используется PSK, парольная фраза PSK преобразуется в 256-битное значение, необходимое для парного главного ключа. В режиме PSK для управления ключами шифрования используется 4-стороннее установление связи, определяемое стандартом 802.11i, без обмена EAP. Поскольку отсутствует сервер RADIUS и методы EAP (EAP-TLS, LEAP), режим PSK менее безопасен.



Supplicant (STA)	Проситель (станция)
Authenticator (AP)	Аутентификатор (точка доступа)
Authentication Server (AS)	Сервер аутентификации
AS sends the pairwise master key…	Сервер аутентификации передает парный главный ключ аутентификатору (точке доступа) по своему безопасному каналу
Key	Ключ
Secure Channel…	Безопасный канал (например, RADIUS с MPPE)

Процедура четырехэтапного установления связи выполняет обмен ключами для работы в режиме предварительного совместно используемого ключа (точка доступа аутентификатора и сервер аутентификации AS находятся непосредственно на точке доступа)

PSK используется для устранения необходимости настраивать сервер аутентификации (RADIUS), но имеет более низкую безопасность. Спецификация 802.11i указывает, что безопасность может считаться слабой, если кодовая фраза включает менее 20 символов, поскольку ее можно легко взломать с помощью атаки по словарю после захвата четырехэтапного установления связи. Проблема в том, что производители не предоставляют никаких простых в использовании инструментов, которые могут генерировать 20-символьные парольные фразы и управлять ими. Смотрите статью Роберта Московица «Слабость при выборе парольной фразы в интерфейсе WPA» (Weakness in Passphrase Choice in WPA Interface) от 4 ноября 2003 года.

Решение AirMagnet

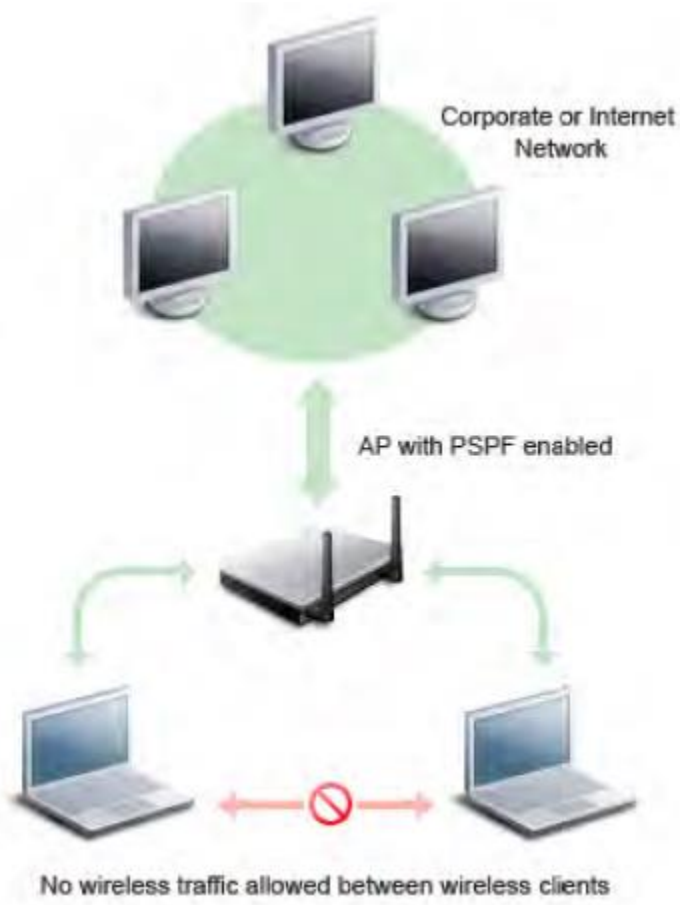
Приложение AirMagnet WiFi Analyzer обнаруживает использование режима PSK и рекомендует переключиться на более безопасную систему управления ключами и аутентификации на основе 802.1x-EAP. Если вы решите использовать управление ключами в режиме PSK, убедитесь, что выбранная вами

кодовая фраза превышает 20 символов и не содержит слов из словаря, что предотвратит возможные атаки.

Publicly Secure Packet Forwarding (PSPF) Violation (Нарушение PSPF (Защищенная пересылка общедоступных пакетов)

Описание сигнала тревоги и возможные причины

PSPF (Publicly Secure Packet Forwarding - Защищенная пересылка общедоступных пакетов) - это функция, реализованная в точках доступа WLAN для блокировки связи беспроводных клиентов с другими беспроводными клиентами. При включенной функции PSPF клиентские устройства не могут взаимодействовать в беспроводной сети с другими клиентскими устройствами.



Corporate or Internet Network	Корпоративная сеть или сеть интернет
AP with PSPF enabled	Точка доступа с включенной функцией PSPF
No wireless traffic allowed…	Не допускается никакой беспроводный трафик между беспроводными клиентами

Функция PSPF защищает общедоступную сеть, запрещая беспроводный трафик между беспроводными клиентами

В большинстве сетей WLAN беспроводные клиенты взаимодействуют только с такими устройствами, как веб-серверы проводной сети. Включение функции PSPF защищает беспроводных клиентов от взлома злоумышленником по беспроводной сети. Функция PSPF (этот термин обычно используется компанией Cisco; другие производители могут называть эту функцию по-другому) эффективна для защиты беспроводных клиентов, особенно в беспроводных общедоступных сетях (публичных точках доступа), например, в аэропортах, отелях, кафе, университетских городках и т.п., где выполняется нулевая аутентификация и любой желающий может подключаться к точкам доступа. Функция PSPF предотвращает непреднамеренный обмен файлами между клиентскими устройствами в беспроводной сети.

Решение AirMagnet

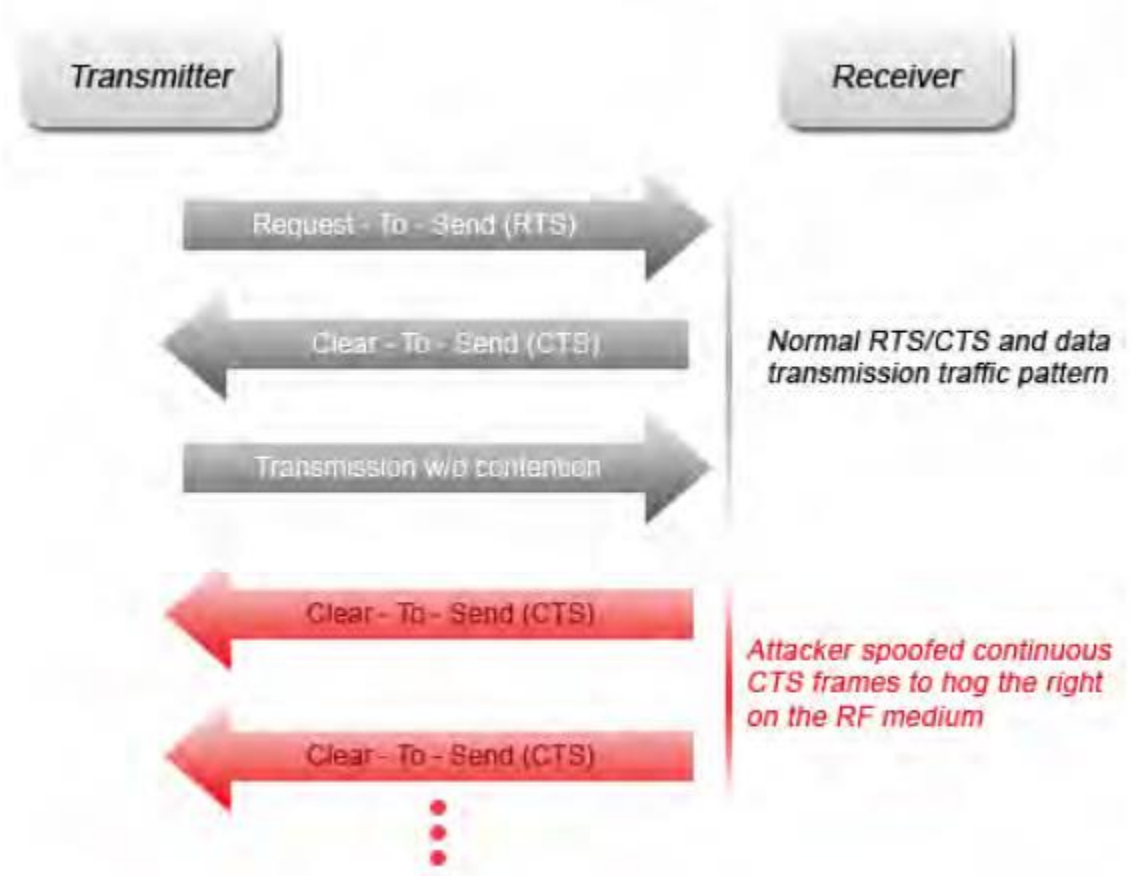
Приложение AirMagnet WiFi Analyzer обнаруживает нарушения PSPF. То есть, если беспроводный клиент пытается связаться с другим беспроводным клиентом, приложение AirMagnet Wi-Fi Analyzer подаст сигнал тревоги о потенциальной атаке вторжения. Этот сигнал тревоги не применяется, если в вашей сети WLAN имеются беспроводные принтеры или используются приложения VoWLAN, потому что эти приложения используют беспроводную связь клиент-клиент.

Denial-of-Service Attack: CTS Flood (Атака типа «отказ в обслуживании»: Флуд CTS)

Инструмент атаки: CTS Jack

Описание сигнала тревоги и возможные причины

Для управления доступом станции к радиочастотной среде в качестве дополнительной функции стандарт IEEE 802.11 использует функцию RTS/CTS (Request-To-Send/Clear-To-Send). Готовое к передаче беспроводное устройство отправляет кадр RTS, чтобы получить право на использования радиочастотной среды в течение определенного периода времени. Приемник удовлетворяет запрос, отправляя кадр CTS той же длительности. Все беспроводные устройства, наблюдающие кадр CTS, должны уступить среду передатчику для осуществления передачи без конкуренции. Хотя этот метод помогает снизить сетевой трафик, он оставляет вашу сеть уязвимой для конкретной DoS-атаки, в которой хакер повторно передает поддельные кадры CTS. Эти кадры информируют другие устройства о том, что сеть используется, и поэтому другой трафик должен ждать. Смотрите рисунок ниже.



Transmitter	Передатчик
Receiver	Приемник
Request-to-Send (RTS)	Готовность к передаче
Clear-to-Send (CTS)	Готовность к приему
Normal RTS/CTS and data transmission…	Нормальный шаблон передачи трафика для RTS/CTS и данных
Transmission w/o contention	Передача без конкуренции

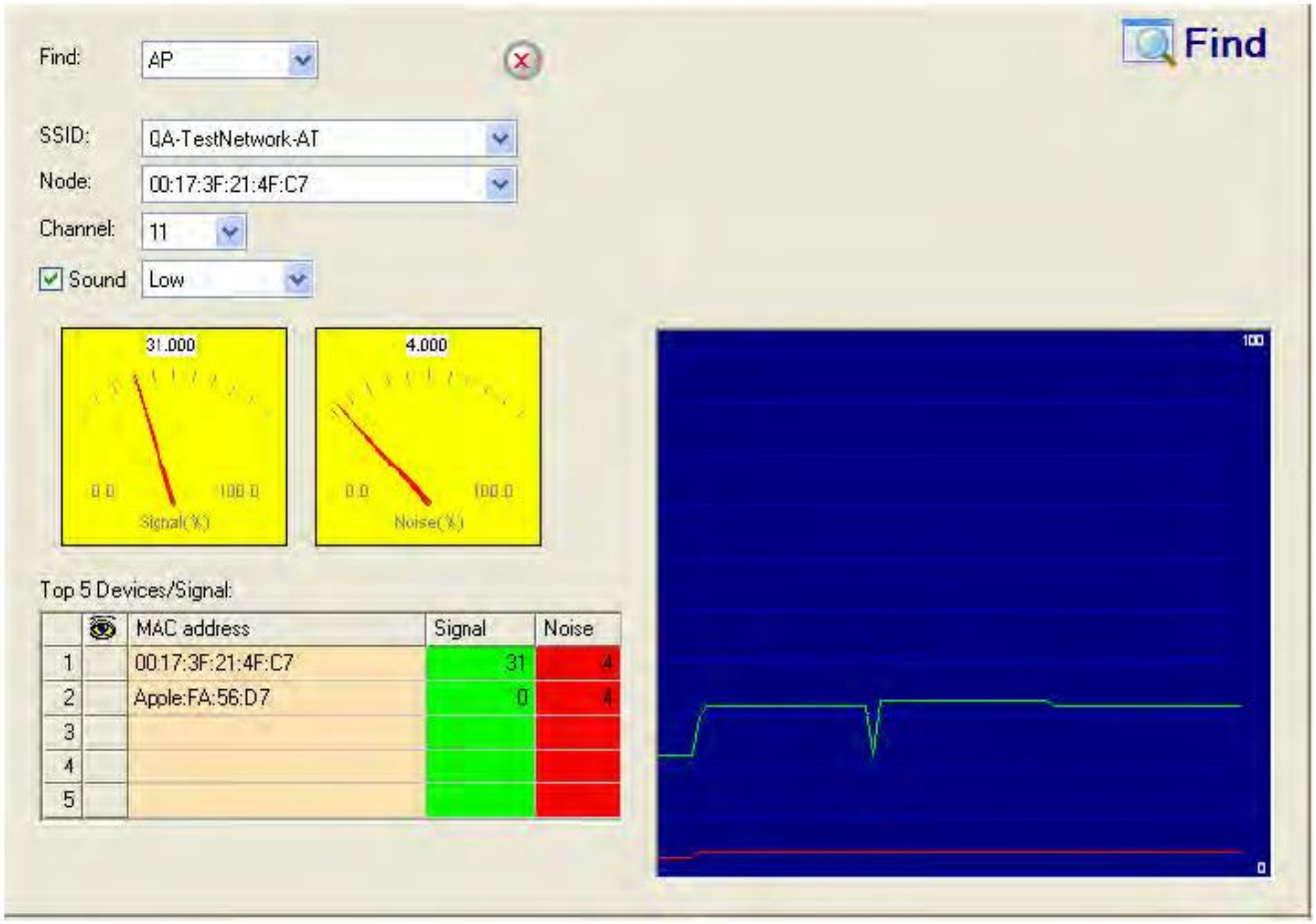
Attacker spoofed continuous CTS frames…	Атакующий подделывает непрерывный поток кадров CTS для захвата права на радиочастотную среду

Стандартный механизм обмена кадрами RTS/CTS и DoS-атаки с внедрением злоумышленником поддельных кадров CTS

Проводящий DoS-атаку злоумышленник может воспользоваться предоставляемой кадру CTS привилегией, чтобы зарезервировать радиочастотную среду для передачи. С помощью последовательной передачи кадров CTS злоумышленник может заставить другие беспроводные устройства, совместно использующие радиочастотную среду, сдерживать свою передачу до тех пор, пока злоумышленник не перестанет передавать кадры CTS.

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает злоупотребление кадрами CTS для проведения атаки типа «отказ в обслуживании». Как и при атаке радиочастотных помех, сотрудники службы безопасности могут использовать инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer для определения источника избыточных кадров CTS.

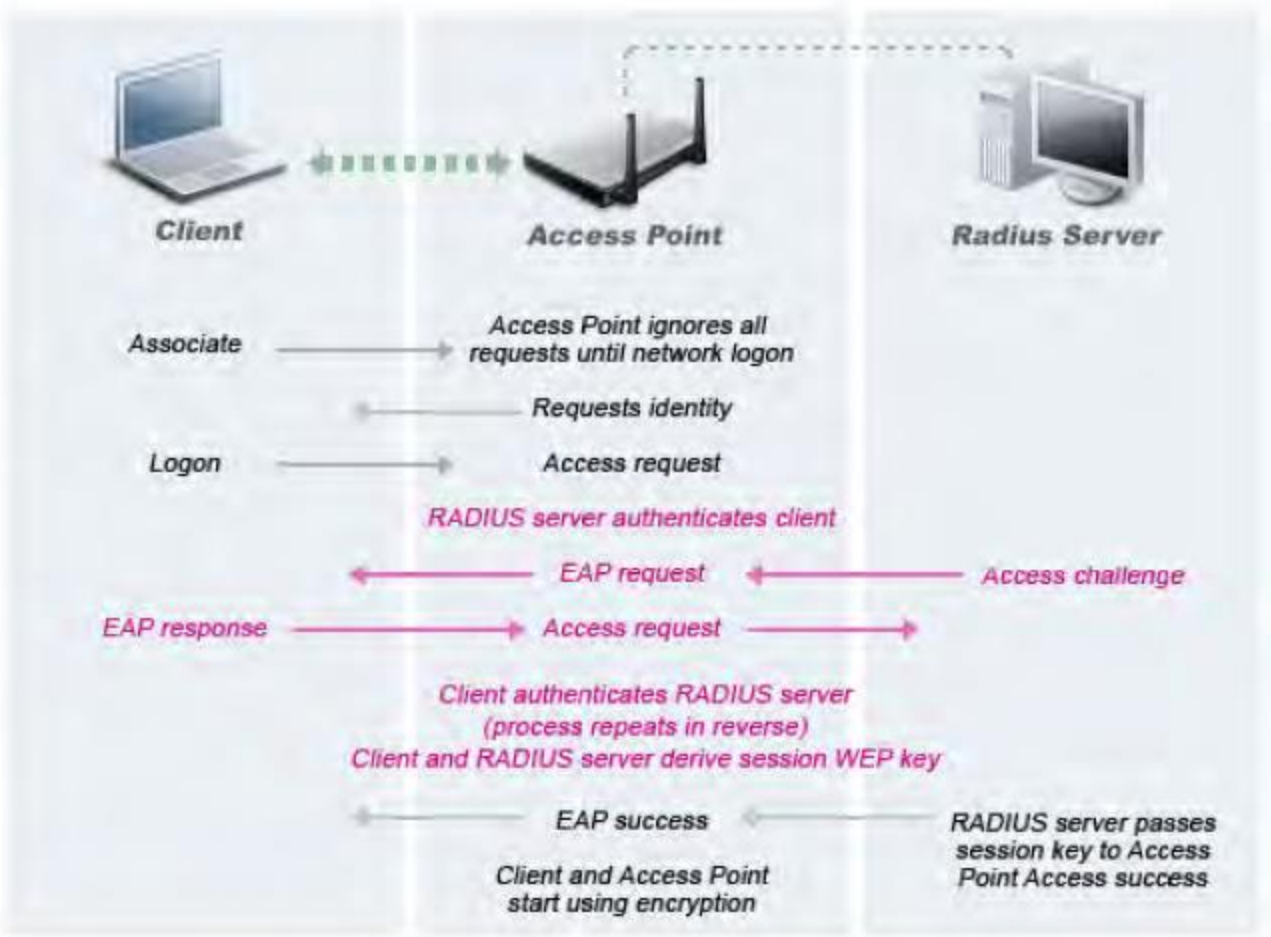


Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает злоумышленников, отслеживая уровень их сигнала

802.1x Unencrypted Broadcast or Multicast (Незашифрованная широковещательная или многоадресная передача 802.1x)

Описание сигнала тревоги и возможные причины

Для защиты от уязвимостей, унаследованных от глобального механизма статических ключей WEP, структура 802.1x позволяет системе использовать ключи шифрования для каждого сеанса. Кроме того, 802.1x также упрощает механизм ротации ключей сеанса, тем самым обеспечивая периодическое обновление ключей шифрования. Это повышает безопасность за счет устранения использования статических ключей шифрования и предотвращения атак, требующих сбора больших объемов данных, зашифрованных с помощью одного статического ключа.



Client	Клиент
Access Point	Точка доступа
Radius Server	Сервер Radius
Associate	Подключение
Access Point ignores all requests…	Точка доступа игнорирует все запросы до входа в сеть
Requests Identity	Запрос идентичности
Logon	Вход
Access request	Запрос доступа
RADIUS server authenticates client	Сервер RADIUS аутентифицирует клиента
EAP request	Запрос EAP
Access challenge	Требование доступа
EAP response	Ответ EAP
Access request	Запрос доступа
Client authenticates RADIUS server…	Клиент аутентифицирует сервер RADIUS (процесс повторяется в обратном порядке). Клиент и сервер RADIUS создают ключ WEP для сеанса.
EAP success	Успешная аутентификация EAP

RADIUS server passes session key…	Сервер RADIUS передает ключ сеанса на точку доступа. Доступ выполнен успешно.
Client and Access Point…	Клиент и точка доступа начинают использовать шифрование

Протокол обмена ключами 802.1x передает ключ шифрования для каждого сеанса на точку доступа и клиентскую станцию.

Для многоадресных и широковещательных пакетов, имеющих несколько получателей, нельзя применить ключ шифрования для каждого сеанса. Для защиты многоадресной и широковещательной передачи необходимо реализовать совместно используемый ключ шифрования и механизм смены ключей. Было обнаружено, что очень немногие беспроводные устройства правильно реализуют механизм многоадресного и широковещательного ключа шифрования. В действительности, многоадресные и широковещательные пакеты, как правило, вообще не шифруются. Чтобы усложнить ситуацию, точки доступа корпоративного уровня с несколькими идентификаторами SSID часто развертываются с безопасностью 802.1x для одного идентификатора SSID (корпоративная сеть WLAN) и без шифрования для другого идентификатора SSID (гостевая сеть WLAN). Этот сценарий развертывания обычно связан с конфигурацией VLAN, поэтому клиентские устройства, использующие гостевой SSID, могут получить доступ только к сети Интернет, но не к корпоративной проводной сети. Поддерживающая несколько идентификаторов SSID точка доступа передает широковещательные и многоадресные кадры, что усложняет выбор варианта шифрования (802.1x или без шифрования).

Решение AirMagnet

Приложение AirMagnet WiFi Analyzer обнаруживает незашифрованные кадры многоадресной и широковещательной рассылки, вызванные неправильной настройкой конфигурации или ошибками реализации производителя. AirMagnet рекомендует использовать точки доступа, которые надлежащим образом реализуют шифрование многоадресных и широковещательных кадров.

Rogue AP by Channel (Неавторизованная точка доступа на канале)

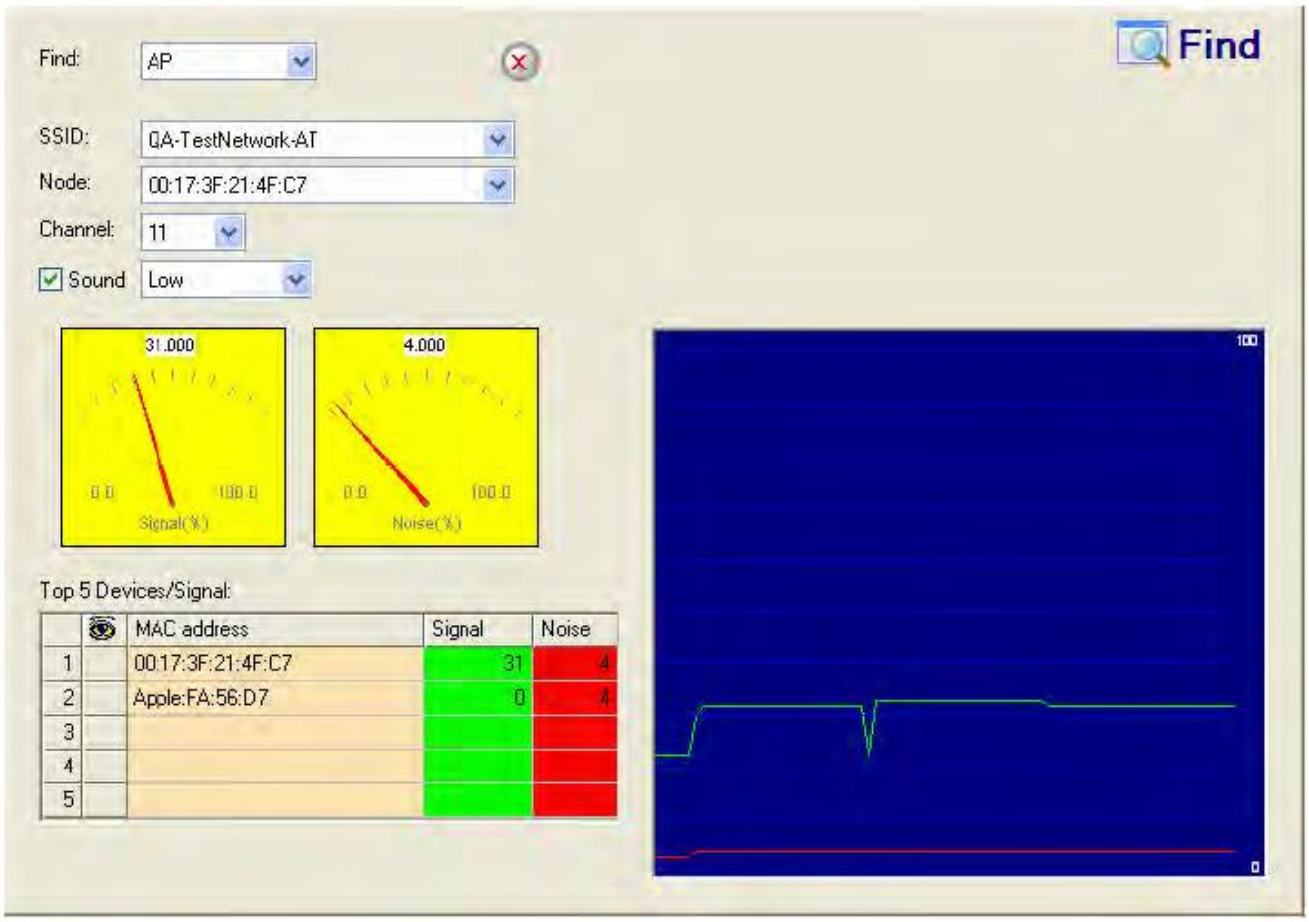
Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer предупреждает администратора сети WLAN о неавторизованных точках доступа, проводя проверку на соответствие стандартизированным корпоративным назначениям рабочих радиочастотных каналов для стандартов 802.11a, 802.11b или 802.11g. Если приложение AirMagnet WiFi Analyzer обнаруживает точку доступа, работающую в стандартизованном радиоканале, не используемом в корпоративной сети, то подаст сигнал тревоги о неавторизованной точке доступа.

Неавторизованные точки доступа, установленные неавторизованными сотрудниками, обычно не соответствуют стандартным корпоративным методам развертывания и, таким образом, могут поставить под угрозу безопасность беспроводных и проводных сетей. Мошенническая точка доступа также может указывать на то, что проводную сеть предприятия пытается взломать злоумышленник. Обнаруженные приложением AirMagnet WiFi Analyzer неавторизованные устройства необходимо тщательно исследовать.

Решение AirMagnet

После того, как приложение AirMagnet WiFi Analyzer обнаружило неавторизованную точку доступа и подало сигнал тревоги, администратор WLAN может использовать инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer для определения местоположения неавторизованного устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Rogue Station by Channel (Неавторизованная станция на канале)

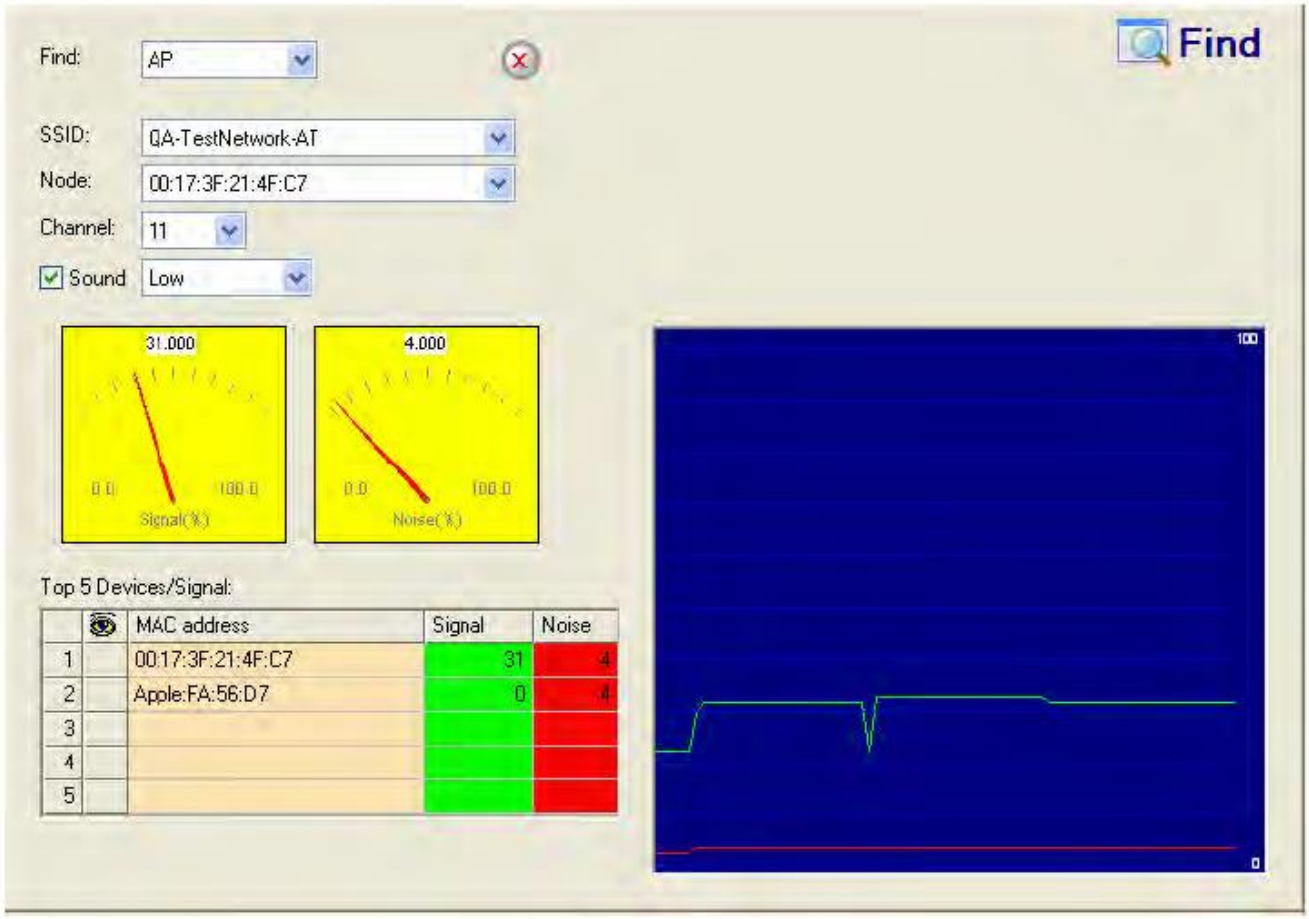
Описание сигнала тревоги и возможные причины

Приложение AirMagnet WiFi Analyzer предупреждает администратора сети WLAN о неавторизованных станциях, проводя проверку на соответствие стандартизированным корпоративным назначениям рабочих радиочастотных каналов для стандартов 802.11a, 802.11b или 802.11g. Если приложение AirMagnet WiFi Analyzer обнаруживает станцию, работающую в стандартизованном радиоканале, не используемом в корпоративной сети, то подаст сигнал тревоги о неавторизованной станции.

Неавторизованные станции, установленные неавторизованными сотрудниками, обычно не соответствуют стандартным корпоративным методам развертывания и, таким образом, могут поставить под угрозу безопасность беспроводных и проводных сетей. Мошенническая станция также может указывать на то, что проводную сеть предприятия пытается взломать злоумышленник. Обнаруженные приложением AirMagnet WiFi Analyzer неавторизованные устройства необходимо тщательно исследовать.

Решение AirMagnet

После того, как приложение AirMagnet WiFi Analyzer обнаружило неавторизованную станцию и подало сигнал тревоги, администратор WLAN может использовать инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer для определения местоположения неавторизованного устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Soft AP or Host AP Detected (Обнаружена программная или аппаратная (хост) точка доступа)

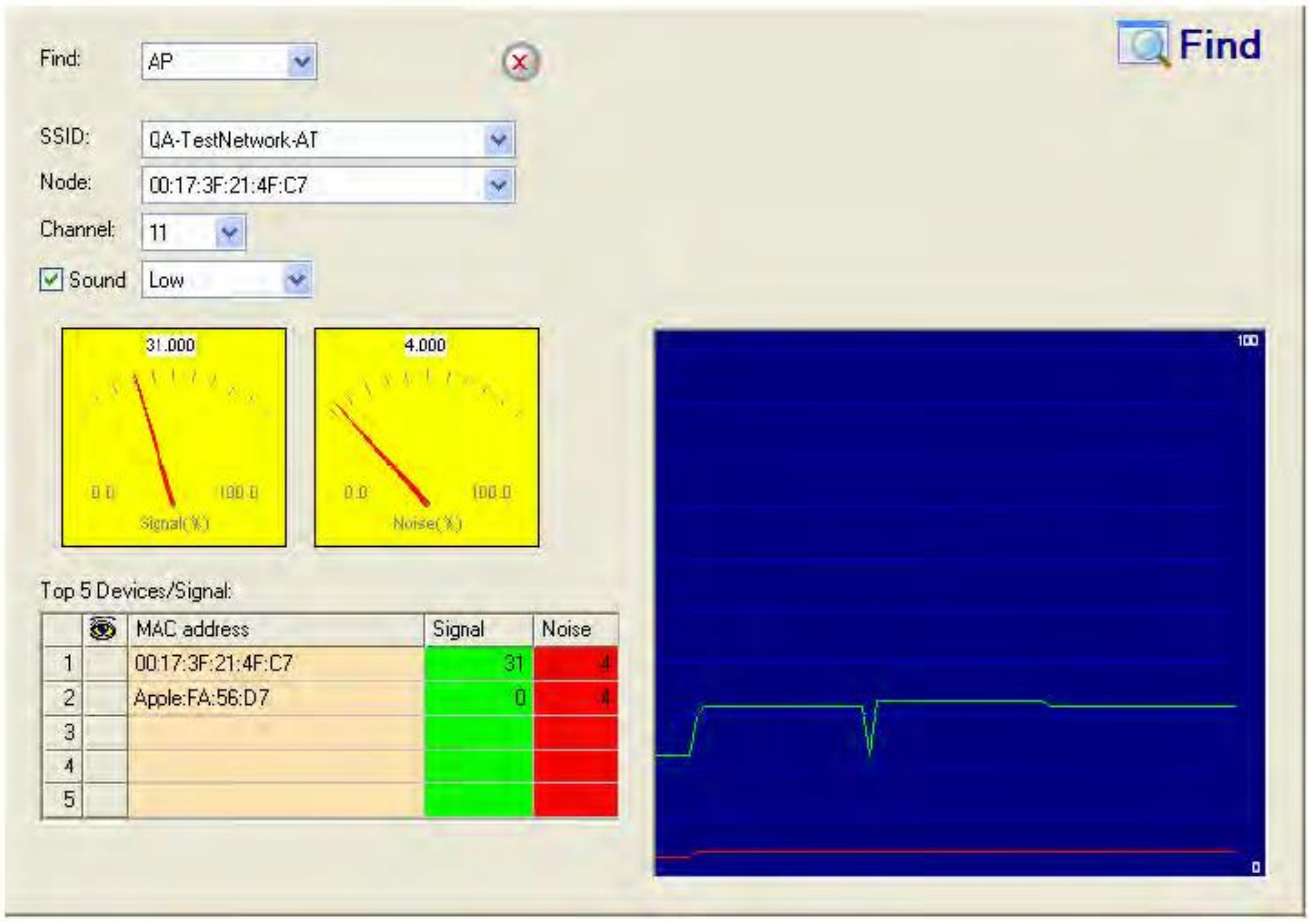
Инструменты Host-AP: Cqure AP

Описание сигнала тревоги и возможные причины

Аппаратная точка доступа (настольный компьютер или портативный компьютер, служащий точкой беспроводного доступа) представляет две потенциальные угрозы безопасности предприятия. Во-первых, аппаратные точки доступа не являются частью инфраструктуры корпоративной беспроводной сети и, скорее всего, являются мошенническими устройствами, не соответствующими корпоративной политике безопасности. Во-вторых, они могут использоваться злоумышленниками в качестве удобной платформы для реализации различных известных вторжений, таких как «человек посередине», точка доступа «honey-pot», имитация точки доступа, атаки типа «отказ в обслуживании» и т.д. Поскольку программные инструменты для превращения настольного или портативного компьютера в точку доступа можно легко загрузить из сети Интернет, аппаратные точки доступа представляют собой нечто большее, чем просто теоретическую угрозу. Кроме того, некоторые ноутбуки поставляются с предварительно загруженным и активированным программным обеспечением HostAP. Как только эти ноутбуки подключаются к корпоративной беспроводной сети, они становятся уязвимыми для хакеров.

Решение AirMagnet

Любая обнаруженная приложением AirMagnet WiFi Analyzer, программная точка доступа должна рассматриваться как мошенническая, а также как потенциальная попытка вторжения. После того, как программная точка доступа идентифицирована и от приложения AirMagnet WiFi Analyzer получено предупреждение, администратор WLAN может использовать инструмент FIND (Найти) для поиска неавторизованного устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Безопасность IDS/IPS

Добавление беспроводной сети WLAN в корпоративную среду формирует новый класс угроз сетевой безопасности. Радиочастотные сигналы, которые проникают через стены и выходят за намеченные границы, могут сделать сеть доступной для неавторизованных пользователей. Неавторизованные точки доступа, установленные сотрудниками для личного использования, обычно не соответствуют корпоративной политике безопасности. Одна неавторизованная точка доступа может подвергнуть всю корпоративную сеть риску проникновения извне и атак. Кроме того, существует множество других возможных рисков и вторжений для безопасности беспроводной сети, таких как неправильно настроенная точка доступа, ненастроенная точка доступа и атаки типа «отказ в обслуживании».

Default Settings	Настройки по умолчанию
Unique SSID with…	Уникальный идентификатор SSID с отключенной его широковещательной рассылкой
Sharев Key…	Аутентификация с помощью совместно используемого ключа с WEP

Open Authentication…	Открытая аутентификация с WEP
MAC Based…	Аутентификация на основе MAC-адреса с WEP
EAP Authentication with WEP	Аутентификация EAP с WEP
EAP Authentication with MIC…	Аутентификация EAP с широковещательной рассылкой MIC, ротацией ключей и WEP
Simple	Проще
Complex	Сложнее

Методы беспроводной безопасности

Приложение AirMagnet WiFi Analyzer разработано для оказания помощи в борьбе с угрозами безопасности путем проверки правильных конфигураций безопасности и обнаружения возможных вторжений. Благодаря комплексному набору технологий мониторинга безопасности приложение AirMagnet Wi-Fi Analyzer предупреждает пользователя о более чем 100 различных угрозах в следующих категориях:

- Аутентификация пользователя и шифрование трафика
- Неавторизованные устройства и устройства ad-hoc
- Уязвимости конфигурации
- Обнаружение вторжений при проникновении в систему безопасности
- Обнаружение вторжений при атаках типа «отказ в обслуживании»

Для максимального использования возможностей приложения AirMagnet WiFi Analyzer сигналы нарушения безопасности можно настроить в соответствии с вашей политикой сетевой безопасности. Например, если ваша сеть WLAN включает в себя точки доступа, изготовленные конкретным производителем, приложение AirMagnet WiFi Analyzer можно настроить для подачи сигнала тревоги о неавторизованной точке доступа при обнаружении точки доступа, изготовленной другим производителем.

Нарушение производительности

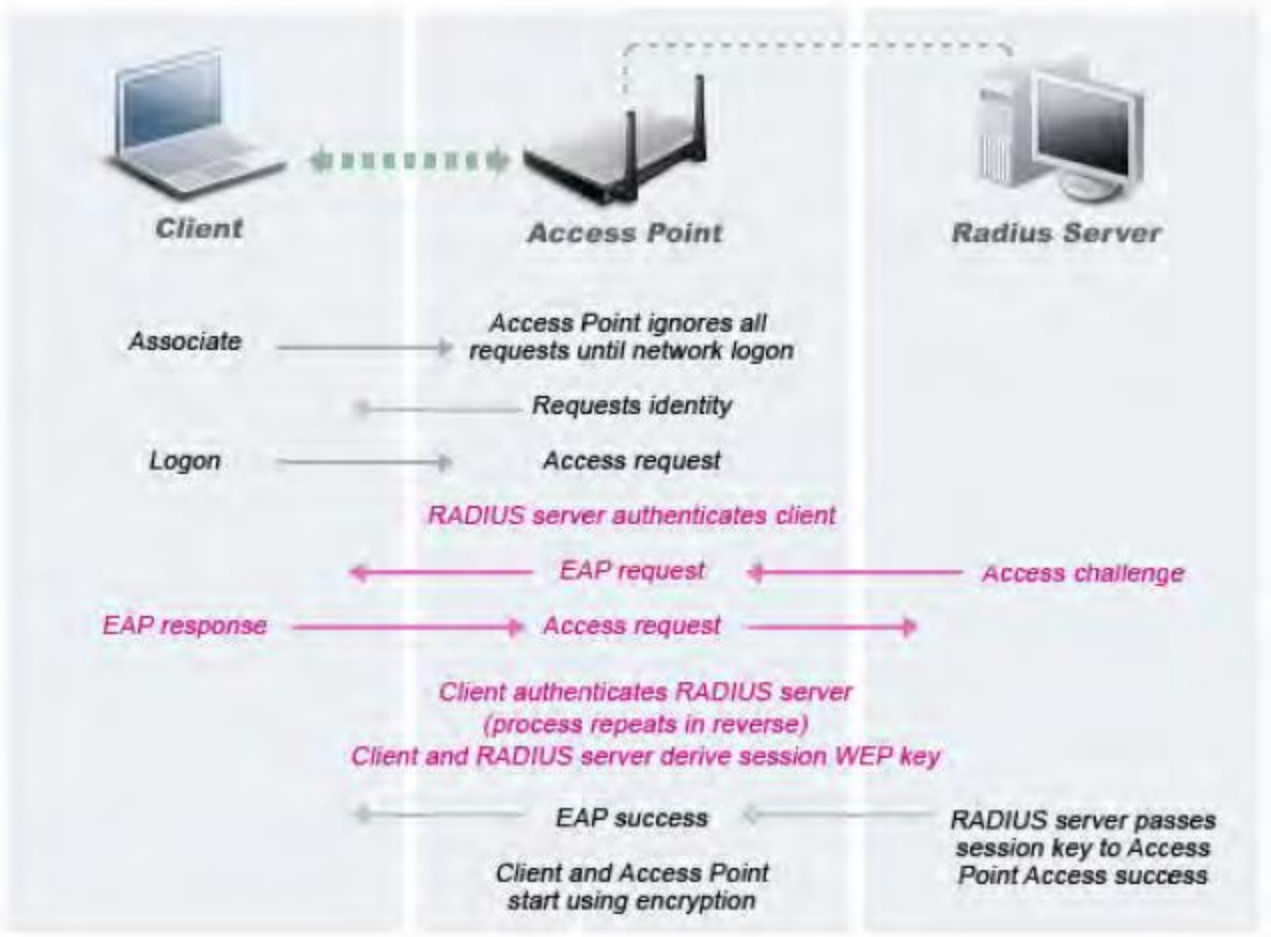
Динамика радиочастотной среды и мобильность клиентских устройств постоянно подвергает испытаниям эффективность работы сети WLAN. Тщательно контролируемая и хорошо настроенная система WLAN способна обеспечить более высокую пропускную способность по сравнению с плохо управляемой сетью. Приложение AirMagnet WiFi Analyzer предоставляет инструмент для обследования площадки, который помогает провести точное развертывание и установку сети WLAN. Приложение AirMagnet Wi-Fi Analyzer обеспечивает лучшую производительность и эффективность сети WLAN, отслеживая сеть и предупреждая администратора беспроводной сети о ранних признаках неисправности. В случае любого ухудшения производительности подаются сигналы тревоги, которые классифицируются по следующим категориям:

- Радиочастотное управление
- Шаблоны проблемного трафика
- Перегрузка канала или устройства
- Ошибка развертывания и эксплуатации
- Проблемы с IEEE 802.11e и VoWLAN

Для максимального использования возможностей приложения AirMagnet Wi-Fi Analyzer можно настраивать сигналы тревоги, касающиеся производительности беспроводной локальной сети, в соответствии с ее спецификациями. Например, если ваша сеть WLAN предназначена для использования всеми пользователями только скоростей 5,5 и 11 Мбит/с, можно настроить пороговое значение таким образом, чтобы подавался сигнал тревоги Low speed tx rate exceeded (Превышен нижний предел скорости передачи данных).

Аутентификация пользователя и шифрование трафика

Первой линией защиты безопасности сети WLAN является аутентификация пользователя и шифрование беспроводного трафика. Централизованная аутентификация пользователей сети WLAN на основе стандарта IEEE 802.1x с сервером RADIUS представляет собой гибкий и надежный механизм. На рисунке ниже показан процесс аутентификации 802.1x:



Client	Клиент
Access Point	Точка доступа
Radius Server	Сервер Radius
Associate	Подключение
Access Point ignores all requests…	Точка доступа игнорирует все запросы до входа в сеть
Requests Identity	Запрос идентичности
Logon	Вход
Access request	Запрос доступа
RADIUS server authenticates client	Сервер RADIUS аутентифицирует клиента
EAP request	Запрос EAP
Access challenge	Требование доступа
EAP response	Ответ EAP
Access request	Запрос доступа
Client authenticates RADIUS server…	Клиент аутентифицирует сервер RADIUS (процесс повторяется в обратном порядке). Клиент и сервер RADIUS создают ключ WEP для сеанса.
EAP success	Успешная аутентификация EAP
RADIUS server passes session key…	Сервер RADIUS передает ключ сеанса на точку доступа. Доступ выполнен успешно.
Client and Access Point…	Клиент и точка доступа начинают использовать шифрование

Процесс аутентификации пользователя 802.1x

Для достижения тех же целей также можно использовать и другие методы аутентификации (например, VPN). Аутентификация пользователя позволяет блокировать неавторизованный доступ к вашим проводным и беспроводным ресурсам. Рука об руку с аутентификацией пользователя идет шифрование

трафика, во время которого между точкой доступа и авторизованными пользователями идет обмен зашифрованными данными. Шифрование предотвращает перехват вашего беспроводного трафика злоумышленниками.

Приложение AirMagnet Wi-Fi Analyzer проверяет развертывание системы безопасности сети WLAN, отслеживая соответствие транзакций аутентификации и методов шифрования трафика определенной политике безопасности сети, которую оно узнает из конфигурации политики AirMagnet. Например, приложение AirMagnet WiFi Analyzer генерирует сигнал Device unprotected by PEAP (Устройство, незащищенное с помощью PEAP), если PEAP типа 802.1x EAP является стандартизированным протоколом аутентификации вашего предприятия. Обычно в этой категории (аутентификация и шифрование) встречаются такие нарушения безопасности, как неправильная конфигурация, устаревшее программное обеспечение/прошивка и неоптимальный выбор корпоративной политики безопасности. Приложение AirMagnet Wi-Fi Analyzer предупреждает администратора об этих проблемах и предлагает меры противодействия.

Неавторизованная точка доступа и станция

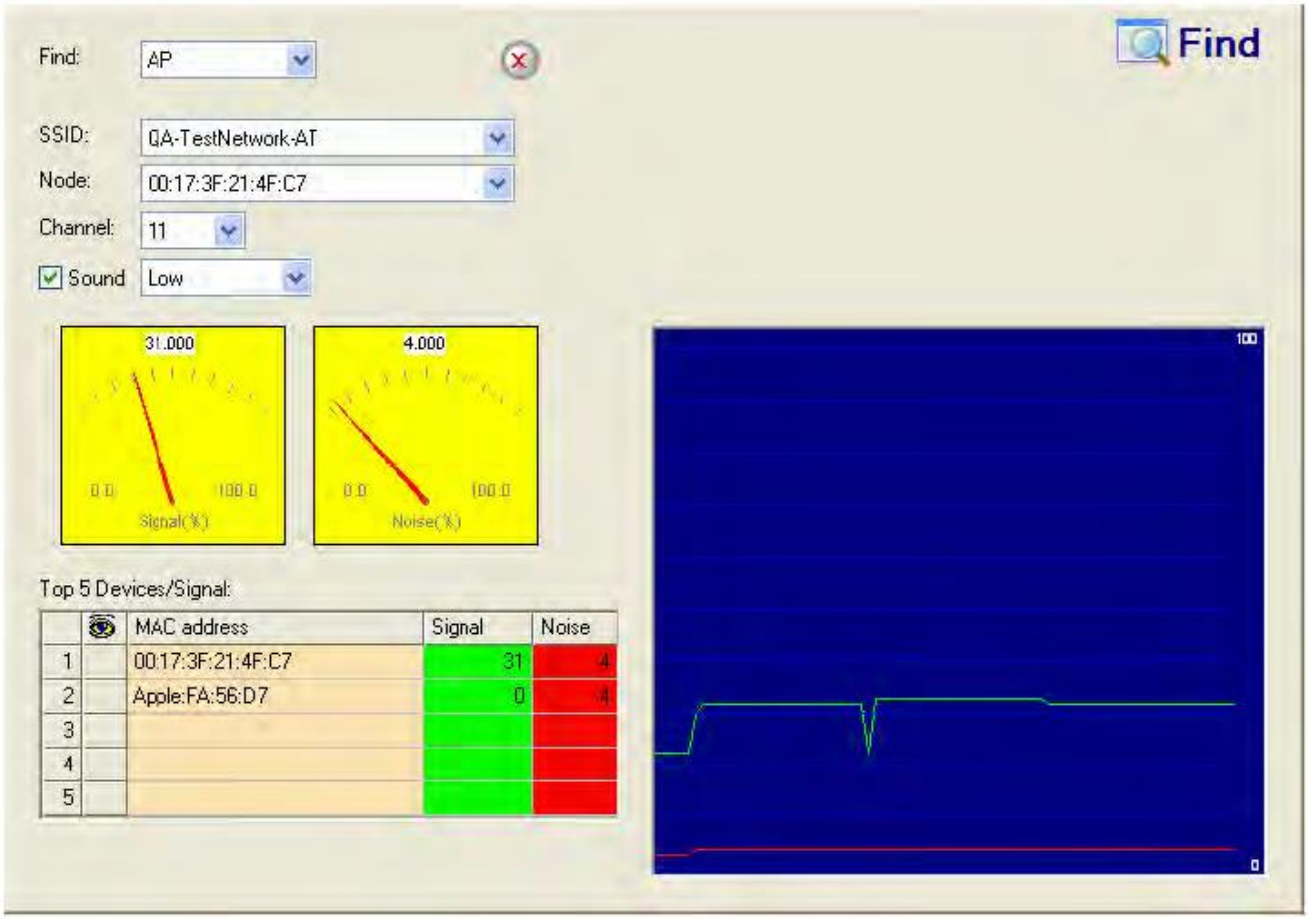
Поскольку технология WLAN набирает популярность в корпоративных и домашних сетях, ИТ-специалисты предприятия часто обнаруживают неавторизованные устройства WLAN, подключенные к корпоративной проводной сети. Эти неавторизованные устройства устанавливаются злоумышленниками или невежественными сотрудниками и обычно не соответствуют политике безопасности корпоративных сетей WLAN, которая требует надежной инфраструктуры аутентификации пользователей и строгих стандартов шифрования трафика. Для защиты целостности беспроводной и проводной корпоративной сети необходимо обнаруживать и немедленно удалять любые неавторизованные устройства.

Приложение AirMagnet Wi-Fi Analyzer предоставляет следующие методы обнаружения неавторизованных устройств. Для определения разницы между авторизованным и неавторизованным устройствами можно использовать любой или несколько из этих методов.

- По MAC-адресу (список контроля доступа)
- По идентификатору производителя оборудования
- По идентификатору SSID
- По типу среды (802.11a/b/g/n)
- По каналу

Например, если в вашей сети WLAN используются только точки доступа Cisco, работающие в режиме 802.11b, эту информацию можно ввести в конфигурацию сигнализации о мошеннических устройствах. Затем приложение AirMagnet WiFi Analyzer будет подавать сигналы тревоги о неавторизованном доступе, если в беспроводной среде будет обнаружена точка доступа другого производителя (не Cisco) или точка доступа 802.11g/n.

После обнаружения неавторизованного устройства и подачи сигнала тревоги приложением AirMagnet Wi-Fi Analyzer администратор сети WLAN сможет воспользоваться инструментом FIND (Найти), чтобы определить местонахождение неавторизованного устройства.



Инструмент FIND (Найти) приложения AirMagnet WiFi Analyzer обнаруживает устройства, отслеживая уровень их сигнала

Уязвимости конфигурации

Реализация строгой политики развертывания имеет определяющее значение для построения безопасной сети WLAN. Однако для соблюдения политики требуется постоянный мониторинг, позволяющий выявлять нарушения, связанные с неправильной настройкой конфигурации или ошибками реализации производителя оборудования. Поскольку все больше и больше ноутбуков поставляются со встроенными возможностями подключения к сети Wi-Fi, конфигурация сети WLAN выходит за рамки точек доступа и станций. Продукты для управления конфигурацией устройств WLAN способны упростить процесс настройки, но необходимость проверки сохраняется, особенно для ноутбуков со встроенным, но неиспользуемым и ненастроенным подключением к Wi-Fi. Помимо проверки соблюдения политик, AirMagnet дает рекомендации по наилучшим методам настройки в случае обнаружения неоптимального выбора конфигурации. Например, приложение AirMagnet WiFi Analyzer подает сигнал предупреждения, когда обнаруживает, что точка доступа транслирует свой идентификатор SSID. Описание сигнала тревоги AirMagnet Wi-Fi Analyzer в этом случае будет рекомендовать администратору беспроводной сети отключить широковещательную передачу SSID в целях обеспечения безопасности.

Обнаружение вторжений - проникновение в систему безопасности

Одной из распространенных форм беспроводного вторжения является нарушение механизма аутентификации WLAN с целью получения доступа к проводной сети или беспроводным устройствам. Атаки на аутентификацию по словарю представляют собой очень распространенную атаку на точку доступа. Злоумышленник также может атаковать беспроводную клиентскую станцию во время процесса ее соединения с точкой доступа. Например, атака с помощью подставной точки доступа на ничего не подозревающего беспроводного клиента может обманом заставить клиента установить связь с этой фейковой точкой доступа. Подобная атака позволяет злоумышленнику получить сетевой доступ к беспроводной станции и потенциально взломать ее файловую систему. Затем злоумышленник может использовать станцию для получения доступа к проводной корпоративной сети.

Подобные угрозы безопасности можно предотвратить, если использовать методы взаимной аутентификации и надежного шифрования. Приложение AirMagnet Wi-Fi Analyzer ищет слабые места в системе безопасности, а также любые попытки проникновения в сеть. AirMagnet WiFi Analyzer обеспечивает надежную защиту беспроводной сети за счет использования наилучшей реализации политики безопасности, а также обнаружения попытки вторжения. При обнаружении подобных уязвимостей или попыток атак приложение AirMagnet WiFi Analyzer генерирует сигналы тревоги, уведомляя администратора о попытках вторжения.

Обнаружение вторжений - Атака «отказ в обслуживании»

Атаки типа «отказ в обслуживании» (DoS-атаки) нацелены на нарушение работы беспроводных служб за счет использования различных уязвимостей сетей WLAN на первом и втором уровнях. DoS-атаки могут быть нацелены на физическую радиочастотную среду, точки доступа, клиентские станции или внутренние серверы аутентификации RADIUS. Например, атака радиочастотных помех с помощью направленной антенны высокой мощности может осуществляться снаружи офисного здания. В используемых злоумышленниками инструментах атаки применяются такие методы взлома, как подделка кадров управления 802.11, подделка кадров аутентификации 802.1x или простое использование метода лавинной передачи пакетов.

Объектами некоторых из этих атак является сама природа и протоколы стандарта беспроводной связи. К счастью, теперь производителям оборудования для сетей WLAN известно о подобных атаках, и для решения этих проблем они разрабатывают новые стандарты, такие как 802.11i. Приложение AirMagnet Wi-Fi Analyzer вносит свой вклад в это решение, предоставляя систему раннего обнаружения, позволяющую сопоставить сигнатуры атак. Обнаружение приложением AirMagnet WiFi Analyzer DoS-атак фокусируется на первом (физическом) и втором уровнях WLAN (уровень канала передачи данных, 802.11, 802.1x). Если используются надежные механизмы аутентификации и шифрования WLAN, DoS-атаки более высокого уровня (уровень IP и выше) становятся трудновыполнимыми. Приложение AirMagnet WiFi Analyzer усиливает защиту WLAN, обеспечивая строгие политики аутентификации и шифрования с помощью своих технологий AirWISE. Кроме того, функция обнаружения DoS-атак и проникновения в систему безопасности приложения AirMagnet WiFi Analyzer обеспечивает круглосуточный непрерывный мониторинг потенциальных беспроводных атак.

Радиочастотное управление

Приложение AirMagnet WiFi Analyzer контролирует физическую радиочастотную среду, динамическую по своей природе и очень часто являющуюся источником проблем с производительностью сети WLAN. Благодаря этому технология AirWISE характеризует следующие основные принципы WLAN и соответствующие сообщения о проблемах:

- Межканальные помехи и проблемы с распределением каналов
- Шумы в канале и сигналы, не относящиеся к стандарту 802.11
- Зона недостаточного радиочастотного покрытия услуг WLAN
- Классический синдром скрытого радиочастотного узла
- Многие другие...

Помимо сложных технических проблем с радиочастотами необходимо соблюдать нормативные правила, устанавливаемые регулирующими органами (такими как FCC, ETSI, TELEC и т.д. – смотрите таблицу ниже). Успешная работа сети WLAN должна быть не только в пределах границ, определяемых регулирующим органом, но также должна учитывать технические вопросы.

Номер канала	Частота (ГГц)	Северная Америка/ ANZ	Европа/ EMEA	Франция/ Сингапур	Испания	Мексика	Израиль	Китай	Япония
1	2412	●	●	●				●	●
2	2417	●	●	●				●	●
3	2422	●	●	●			●	●	●
4	2427	●	●	●			●	●	●
5	2432	●	●	●			●	●	●
6	2437	●	●	●			●	●	●
7	2442	●	●	●			●	●	●
8	2447	●	●	●			●	●	●
9	2452	●	●	●				●	●
10	2457	●	●	●	●	●		●	●
11	2462	●	●	●	●	●		●	●
12	2467		●	●					●
13	2472		●	●					●
14	2484								●
Максимальная мощность (мВт)		100	100				100	5	50

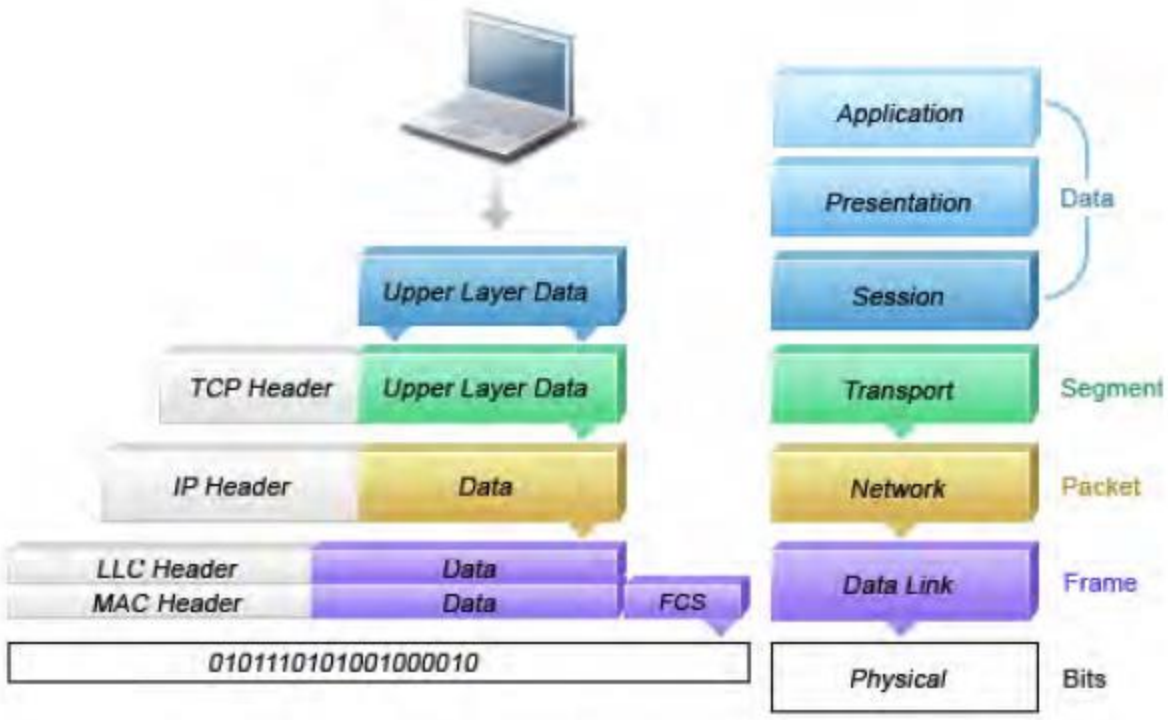
Нормативные правила использования спектра радиочастот 2,4 ГГц по распределению каналов и выходной мощности в разных странах мира.

Примечание: Обратите внимание, что использование канала, проблемы с модуляцией 802.11a/b/g и проблемы протокола уровня MAC классифицируются в категориях производительности приложения AirMagnet Wi-Fi Analyzer, а не в категории радиочастотного управления.

Шаблон проблемного трафика

Многие проблемы производительности сети WLAN (включая проблему многолучевого распространения радиочастотных сигналов) проявляются в транзакциях и статистике протокола уровня MAC. Отслеживая и анализируя беспроводной трафик, приложение AirMagnet WiFi Analyzer позволяет обнаруживать неэффективность и снижение производительности на ранней стадии. Во многих случаях приложение AirMagnet Wi-Fi Analyzer даже способно определить причину появления обнаруженной проблемы с производительностью и предложить необходимые меры противодействия. Приложение AirMagnet WiFi Analyzer отслеживает характеристики протокола уровня MAC, включая следующее:

- Кадровые ошибки CRC
- Повторная передача кадра
- Использование и распределение кадровой скорости (1, 2, 5.5, 11, ... Мбит/с)
- Фрагментация кадра 2-го уровня
- Взаимосвязь соединения/повторного соединения/разъединения между точкой доступа и станцией
- Передача обслуживания в роуминге
- Многие другие...



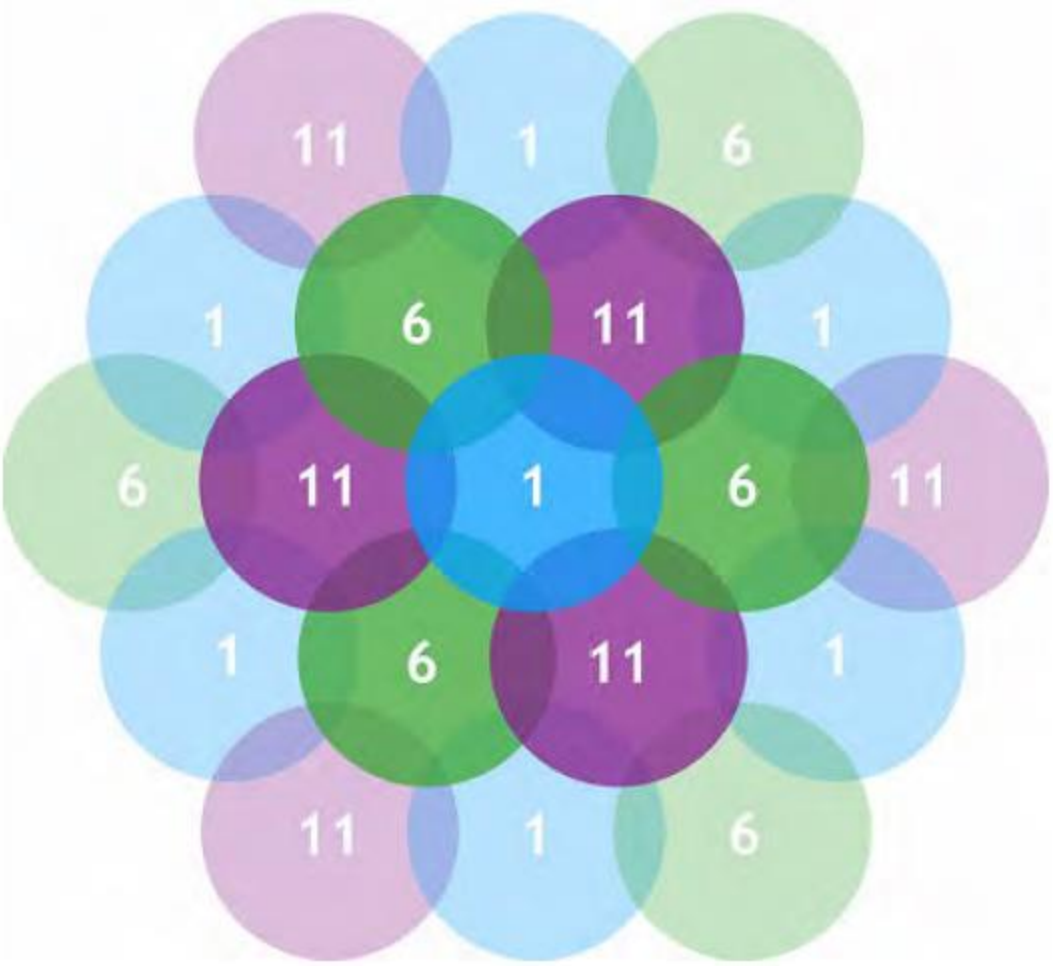
Application	Приложение
Presentation	Презентация
Session	Сеанс
Data	Данные
Upper Layer Data	Данные верхнего уровня
TCP Header	Заголовок TCP
Transport	Транспорт
Segment	Сегмент
IP Header	Заголовок IP
Network	Сеть
Packet	Пакет
LLC Header	Заголовок LLC
MAC Header	Заголовок MAC
Data Link	Канал передачи данных
Frame	Кадр
Physical	Физический уровень
Bits	Биты

Формат пакета данных WLAN и инкапсуляция протокола

Приложение AirMagnet WiFi Analyzer анализирует первый и второй уровни (физический уровень и уровень канала передачи данных, как показано на рисунке выше) для выявления проблем, которые являются уникальными для функционирования сети WLAN. Также приложение AirMagnet WiFi Analyzer может проводить анализ протокола более высокого уровня (включая IP/TCP/UDP/DHCP), если он не зашифрован.

Перегрузка канала или устройства

Технологии WLAN используют радиочастотный спектр как общую физическую среду, аналогичную оригинальной технологии Ethernet 10 Мбит/с, которая позже превратилась в коммутаторы Ethernet. Даже для новейших стандартов WLAN 802.11a и 802.11g все еще существует потолок общей полосы пропускания 54 Мбит/с. В действительности потолок намного ниже, учитывая необходимые служебные данные протокола MAC, межкадровый интервал, коллизии и случайные задержки передачи.



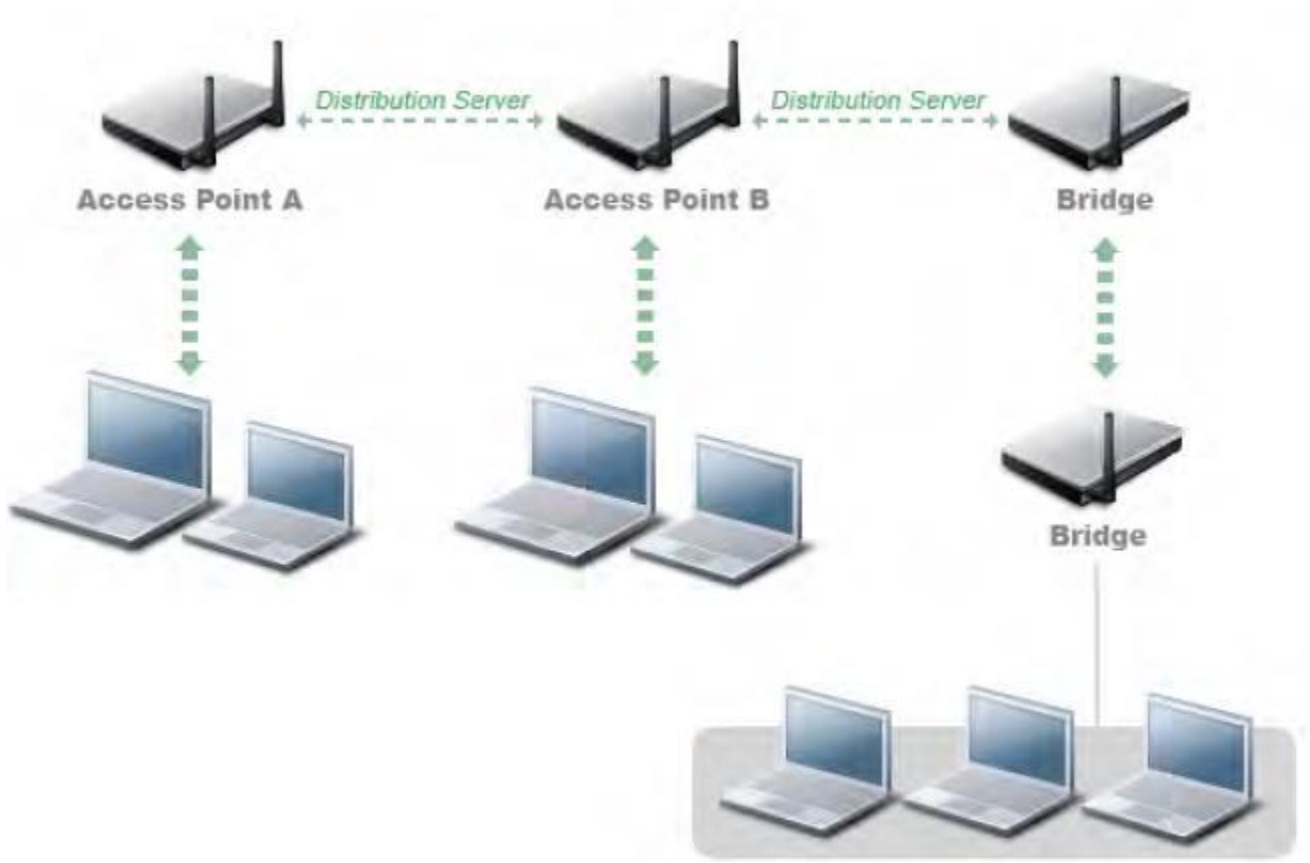
Решающее значение для увеличения пропускной способности WLAN и минимизации помех имеет оптимизированное распределение каналов

Кроме того, что радиочастотная среда имеет ограничения полосы пропускания, точки доступа WLAN имеют ограничения и могут быть перегружены интенсивным трафиком или большим количеством подключенных клиентов. Как и в проводной локальной сети, чрезмерное количество многоадресных и широковещательных кадров способно создать дополнительную нагрузку на устройства WLAN. Перегруженные устройства страдают от снижения производительности и вызывают проблемы с подключением; например, таблица подключения точки доступа может быть переполнена большим количеством клиентов.

Чтобы обеспечить бесперебойную работу сети, приложение AirMagnet WiFi Analyzer контролирует и отслеживает нагрузку, будь то ограничение полосы пропускания канала или ресурс устройства WLAN. Если сеть WLAN не работает удовлетворительно из-за недостаточности ресурсов или чрезмерного роста, приложение AirMagnet WiFi Analyzer выдает сигналы тревоги и предлагает конкретные действия. Следует отметить, что радиочастотная среда не имеет четких границ, что может привести к значительному увеличению использования вашего канала WLAN, даже когда ваш сосед устанавливает новые устройства WLAN на соседнем канале. Приложение AirMagnet Wi-Fi Analyzer контролирует вашу сеть WLAN, гарантируя надлежащую пропускную способность и выделение ресурсов.

Ошибка развертывания и эксплуатации

Важной частью обеспечения эффективности и надежности работы WLAN является правильная настройка ее инфраструктуры. Продукты управления конфигурацией беспроводной сети помогают выполнить согласованную настройку конфигурации крупномасштабных сетей; однако влияние выбора параметров конфигурации на радиочастотные характеристики обычно непредсказуемо и может потребовать проверки.



Access Point A (B)	Точка доступа A (B)
Distribution Server	Сервер распределения
Bridge	Мост

Развертывание сети WLAN включает настройку точек доступа, беспроводных мостов и внутренней службы распределения.

Приложение AirMagnet WiFi Analyzer отслеживает эти параметры конфигурации и их взаимодействие на наличие потенциальных ошибок. Кроме того, приложение AirMagnet Wi-Fi Analyzer контролирует радиочастотную среду, чтобы гарантировать надежное беспроводное обслуживание и обеспечить раннее предупреждение о других неисправностях, например, поврежденных антеннах, сбоях электропитания, ошибках реализации и сбросах настроек точек доступа.

Приложение AirMagnet WiFi Analyzer сканирует радиочастотный спектр на наличие ошибок конфигурации и функционирования. Постоянно контролируется следующее:

- Несогласованная конфигурация точек доступа, обслуживающих сеть с одним и тем же идентификатором SSID
- Конфигурация в соответствии с наилучшим опытом
- Проблемы с подключением, вызванные несоответствием конфигурации клиент/точка доступа
- Устройство инфраструктуры WLAN не работает или сброшены его настройки
- Недостатки в реализации устройства WLAN
- Многие другие...

Стандарт IEEE 802.11e и VoWLAN (Voice over Wireless Local Area Network - Передача голоса по беспроводной локальной сети)

Стандарт IEEE 802.11e добавляет функции качества обслуживания (QoS) и поддержку мультимедиа к существующим стандартам беспроводной связи 802.11 a/b/g, сохраняя при этом полную обратную совместимость с ними. Функция QoS очень важна для приложений передачи голоса и видео. Беспроводная локальная сеть имеет более ограниченную полосу пропускания и более высокие служебные данные, чем традиционная проводная сеть Ethernet. Пропускная способность снижается по

ряду причин, включая механизм RTS/CTS, фрагментацию пакетов, повторную передачу пакетов, подтверждения, коллизии и т.д.

Для беспроводных устройств стандартный протокол MAC в IEEE 802.11 был разработан с двумя коммуникационными режимами: DCF (функция распределенной координации) и PCF (функция координации точек). Механизм DCF предполагает ожидание, если кто-то еще осуществляет передачу, что является частью механизма CSMA/CA. Трафик данных в DCF основан на принципе «первым пришел - первым обслужен»: точка доступа имеет такой же приоритет, что и другие станции. Это очень важно для DCF, поскольку количество устройств в BSS увеличивается, а вместе с ним и коллизии.

Механизм PCF обеспечивает передачу данных через механизм опроса. При этом точка доступа управляет передачей кадров на станции и от них. Точка доступа отправляет сигналы маяка, которые содержат все необходимые параметры. Станция может передавать данные в течение периода без конкуренции (Contention Free Period - CFP). Очень мало производителей выпускает оборудование, поддерживающее метод PCF, и метод PCF страдает от непредсказуемых графиков опроса. Также отсутствует какой-либо механизм, с помощью которого станции могут уведомлять точку доступа о любых требованиях QoS.

Станция, которая включает улучшения QoS, обозначается как QSTA (QoS STA), а точка доступа обозначается как QAP (QoS AP). Если станция QSTA связывается с точкой доступа без улучшений QoS, ей по-прежнему точкой доступа могут предоставляться услуги по передаче данных, отличных от QoS.

Стандарт IEEE 802.11e включает два механизма поддержки приложений:

- Расширенный распределенный доступ к каналу (EDCA): Этот механизм доставляет трафик на основе различных пользовательских приоритетов, связанных с каждым MSDU (MAC Service Data Unit блоком данных службы MAC), назначенным на уровнях выше уровня MAC. Различные приоритеты пользователей можно получить, изменив:
  a) количество времени, в течение которого станция определяет, что канал свободен, до отсрочки или осуществления передачи.
  b) длительность конкурентного окна для отсрочки.
  c) время, в течение которого станция может передавать после того, как займет канал.

- Контролируемый HCF доступ к каналу (HCCA): Этот механизм позволяет резервировать возможности передачи (TXOP: временные интервалы, в которые QSTA может передавать кадры) с гибридным координатором (HC: совмещен с QAP). QSTA запрашивает TXOP у HC - как для своих собственных передач, так и для передач от QAP самому себе. Запрос инициируется объектом управления станцией (SME) QSTA. Если запрос принят, HC планирует TXOP как для QAP, так и для QSTA, на основе политики управления доступом. Для передачи от QSTA гибридный координатор HC опрашивает QSTA на основе параметров, предоставленных QSTA во время его запроса. Для передач на QSTA QAP напрямую получает TXOP от гибридного координатора HC и доставляет кадры из очереди в QSTA, опять же на основе параметров, предоставленных QSTA.

Frame Control	Управление кадром
Duration/ID	Продолжительность/идентификатор
Address	Адрес
Sequence Control	Управление последовательностью
QoS Control	Управление QoS
Frame Body	Тело кадра

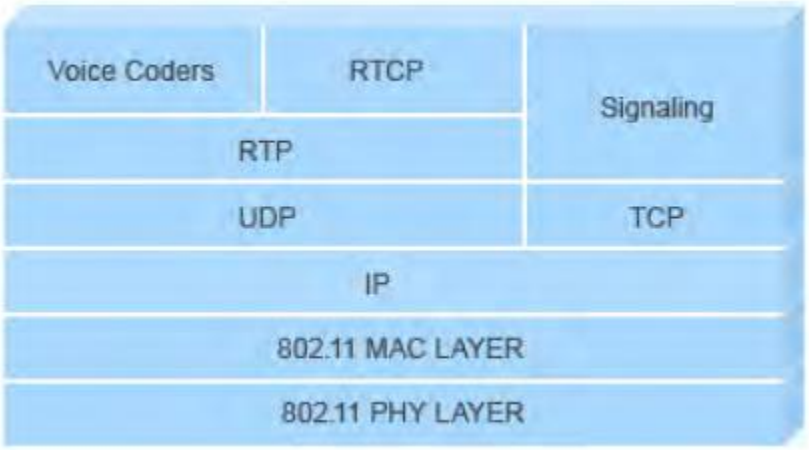
Формат кадра MAC

Следующим «убийственным» приложением для сетей WLAN считается VoWLAN, расширение технологии VoIP. Различными компонентами подобных систем являются:

- Телефон с поддержкой Wi-Fi
- Точка доступа, к которой будет подключен телефон
- На верхних уровнях - система PBX, которая может подключаться к телефонной сети общего пользования (или связь может осуществляться через Интернет).

При развертывании систем VoWLAN необходимо учитывать два наиболее важных момента:

- Емкость: количество телефонов или одновременных вызовов на ячейку сети.
- Роуминг: как сеть справляется с роумингом телефонов от одной точки доступа к другой.



Voice Coders	Голосовые кодеры
Signalling	Сигнализация
802.11 MAC LAYER	Уровень управления доступом к среде 802.11
802.11 PHY LAYER	Физический уровень 802.11

Система VoWLAN с протоколом UDP и уровнями MAC и PHY стандарта 802.11

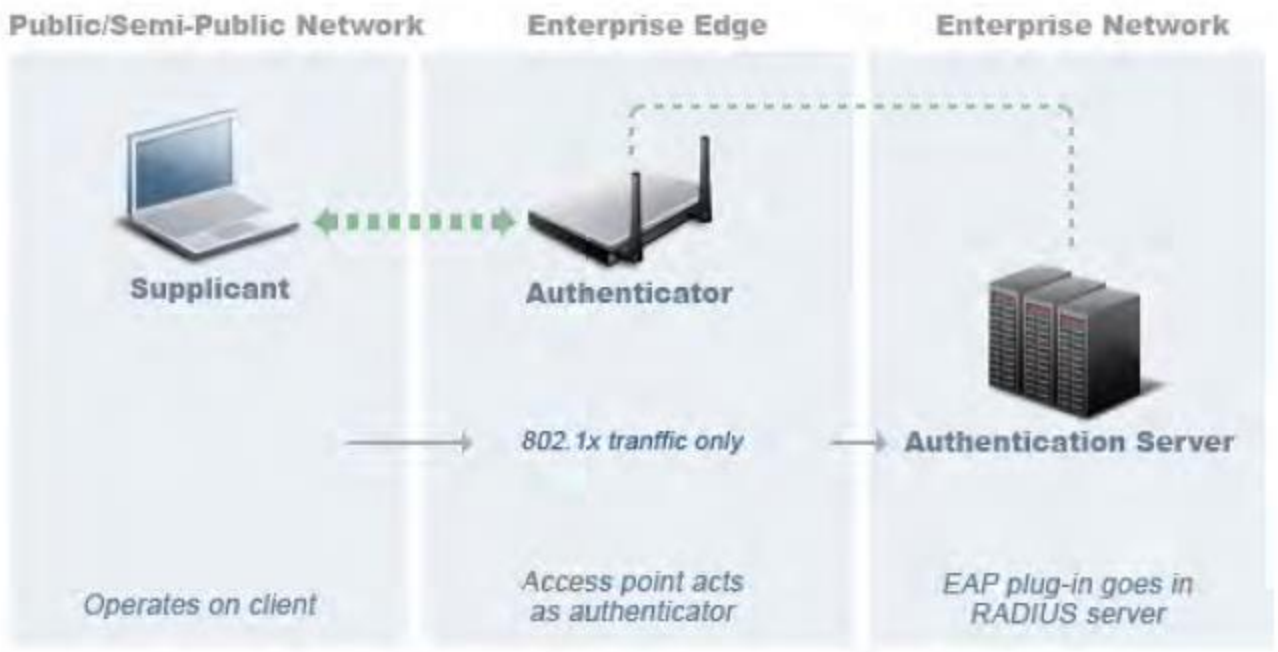
Статическое шифрование WEP

Статическое шифрование WEP было задано в стандарте IEEE 802.11 в 1999 году. С тех пор было опубликовано несколько статей (например, «Weaknesses in the Key Scheduling Algorithm of RC4 – I» (Слабые стороны алгоритма планирования ключей RC4 – I), авторы Scott Fluhrer, Itsik Mantin и Adi Shamir (Скотт Флурер, Ицик Мантин и Ади Шамир)) об уязвимостях этого алгоритма (WEP с использованием RC4 со статическим ключом). Для сетей WLAN, безопасность которых является критическим фактором, для решения задач шифрования существуют такие альтернативы, как WPA (Wireless Protected Access (защищенный беспроводной доступ) - TKIP и 802.1x) и 802.11i.

Интересно, что согласно статистике более 50% сетей WLAN не реализуют какой-либо метод шифрования. Даже с учетом потенциальной уязвимости статического WEP, он все же безопаснее, чем полное отсутствие шифрования. Если вы решите использовать статический WEP, существуют способы сделать его максимально безопасным. Приложение AirMagnet WiFi Analyzer поможет вам в достижении этой цели, отслеживая использование статического WEP и выявляя такие дыры в безопасности, как использование взламываемого ключа WEP и аутентификация с совместно используемым ключом, а также обнаруживая устройства, не использующие WEP.

WPA и 802.11i

Опубликованная Wi-Fi спецификация WPA (Защищенный беспроводный доступ) определяет подмножество функций стандарта IEEE 802.11i. WPA является одним из ответов на широко разрекламированную уязвимость статического WEP, который задается в оригинальной спецификации IEEE 802.11. Большинство поставщиков беспроводных сетей поддерживают WPA и считают его более безопасной альтернативой статическому WEP.



Public/Semi-public Network	Сеть общего пользования
Enterprise Edge	Граница предприятия
Enterprise Network	Сеть предприятия
Supplicant (STA)	Проситель (станция)
Authenticator (AP)	Аутентификатор (точка доступа)
802.1x traffic only	Только трафик 802.1x
Authentication Server (AS)	Сервер аутентификации
Operates on client	Работает на клиенте
Access point acts as authenticator	Точка доступа работает как аутентификатор
EAP plug-in goes in RADIUS server	Плагин EAP на сервере RADIUS

Структура аутентификации и шифрования 802.1x на основе пользователей

Продукты WPA предоставляют конечным пользователям три основных преимущества:
- 802.1x позволяет аутентификацию на основе пользователей вместо уязвимого метода глобального ключа шифрования.
- TKIP (протокол ограниченной по времени целостности ключа) повышает надежность промышленного шифрования с помощью динамического ввода ключей.
- PMK (Pre-shared Master Key) позволяет малым и средним предприятиям использовать 802.1x и TKIP без сложных внутренних инфраструктурных серверов (таких как RADIUS).
- CCMP - это усовершенствованная система шифрования, использующая режим счетчика с протоколом кода аутентификации сообщений (MAC) Cipher Block Chaining (CBC). В CCMP управление ключами и целостность сообщений обрабатываются одним компонентом, построенным на основе AES.

Приложение AirMagnet Wi-Fi Analyzer отслеживает транзакции WPA и предупреждает администратора в случае обнаружения несовместимых устройств и слабых конфигураций.

VPN

Вместо методов аутентификации и шифрования беспроводного уровня 2, таких как 802.1x/EAP, TLS и TKIP (или в дополнение к ним), некоторые сети WLAN для обеспечения надежной безопасности используют технологии VPN уровня 3. В среде с развертыванием VPN приложение AirMagnet WiFi Analyzer обнаруживает устройства, не защищенные такими технологиями VPN, как:
- IPsec - IP-безопасность
- L2TP - протокол туннелирования уровня 2
- PPTP - протокол туннелирования точка-точка
- SSH - безопасная оболочка

Другие методы шифрования и аутентификации

Предложения по обеспечению безопасности приложения AirMagnet WiFi Analyzer охватывают большинство таких стандартных технологий, как WEP, 802.1x, TKIP и VPN. Также приложение поддерживает проприетарные технологии безопасности, развернутые клиентами AirMagnet (такими как Cranite Systems, Inc. и Fortress Technologies, Inc.). По умолчанию эти сигналы тревоги не включены. Если в вашей сети используются какие-либо нестандартные технологии безопасности, следует включить соответствующие сигналы тревоги, чтобы приложение AirMagnet WiFi Analyzer соответствующим образом контролировало вашу сеть.

Неавторизованная точка доступа

Приложение AirMagnet WiFi Analyzer обнаруживает мошеннические (неавторизованные) точки доступа по MAC-адресу, идентификатору производителя, SSID, типу радиочастотной среды и радиочастотным каналам. Для приложения AirMagnet Enterprise датчик AirMagnet можно настроить на автоматический ответ на обнаруженные неавторизованные точки доступа. В таком случае датчик AirMagnet Smartedge Sensor эмулирует беспроводного клиента, используя для связи с неавторизованной точкой доступа объявленный этой точкой идентификатор SSID. После подключения датчик выполняет трассировку уровня IP, чтобы отследить IP-адрес, который используется для входа в проводную сеть вашего предприятия. Этот IP-адрес можно затем использовать для отслеживания порта коммутатора, к которому подключена неавторизованная точка доступа. Отключение порта коммутатора приведет к немедленному отключению неавторизованной точки доступа от корпоративной сети.

Неавторизованная станция

Из-за повсеместного распространения беспроводных устройств (особенно ноутбуков со встроенными картами Wi-Fi) становится все труднее управлять беспроводными клиентами. Неавторизованные станции могут принадлежать злоумышленникам, но также быть и легальными корпоративными компьютерами/ноутбуками, которым не разрешено использовать беспроводные услуги. Неавторизованные беспроводные станции, не соответствующие строгим политикам безопасности предприятия, рискуют раскрыть посторонним важную и конфиденциальную информацию, хранящуюся в системе. Например, висящая неподключенная станция, ищущая беспроводную точку доступа, которая используется в доме сотрудника, рискует подвергнуться атаке со стороны фейковой точки доступа злоумышленника.
Чтобы гарантировать присутствие в вашей сети WLAN только легитимных станций, приложение AirMagnet WiFi Analyzer для обнаружения неавторизованных станций использует тот же механизм, что и для обнаружения неавторизованных точек доступа. Эти механизмы обнаружения основаны на MAC-адресе, идентификаторе производителя, SSID, типе радиочастотной среды и радиочастотных каналах. Кроме того, любая станция, подключившаяся к неавторизованной точке доступа, также вызывает подачу сигнала тревоги о неавторизованной станции.

DoS-атака на точку доступа

DoS-атака (атака типа «отказ в обслуживании») на точки доступа обычно выполняется на основе следующих предположений:

- Точки доступа имеют ограниченные ресурсы. Например, таблица состояния подключения клиентов может содержать только определенное количество записей.
- Кадры управления WLAN и протоколы аутентификации 802.11 и 802.1x не имеют встроенных механизмов шифрования.

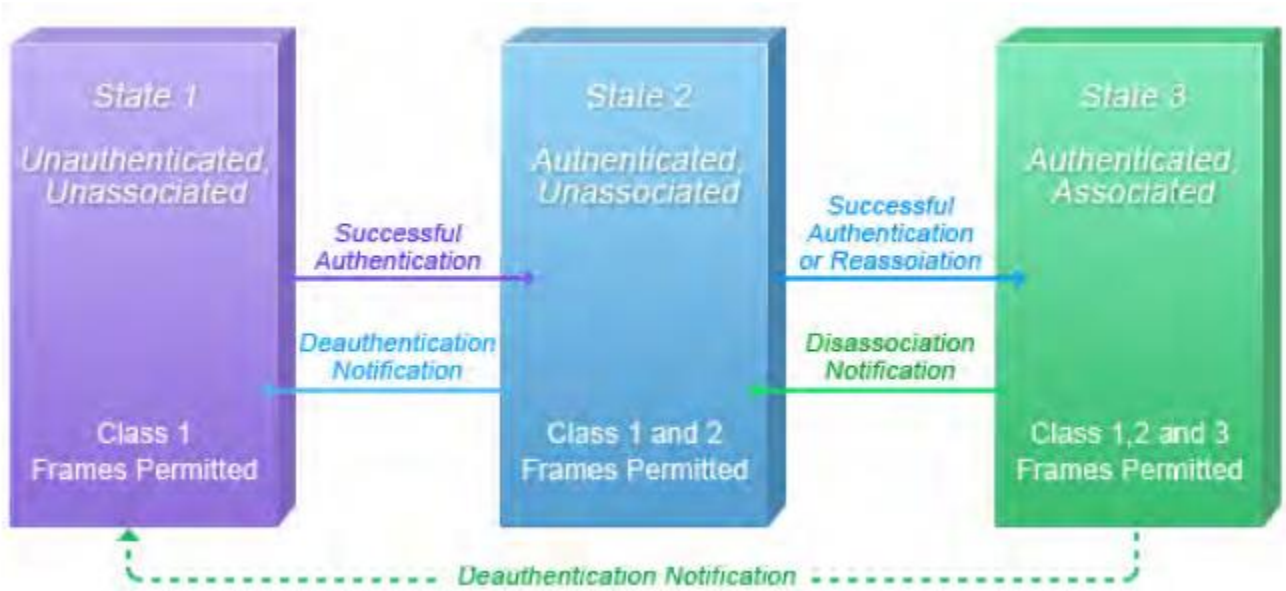
Злоумышленники могут исчерпать ресурсы точки доступа, в первую очередь таблицу подключения клиентов, путем эмуляции большого количества беспроводных клиентов с поддельными MAC-адресами. Каждый из этих эмулируемых клиентов будет пытаться установить связь и пройти аутентификацию с целевой точкой доступа, но остановит обмен протоколами на полпути. После того, как ресурсы точки доступа и таблица подключения клиентов заполнены этими эмулированными клиентами и их незавершенными аутентификациями, легитимные клиенты больше не могут обслуживаться атакуемой точкой доступа. Так формируется атака «отказ в обслуживании».

Приложение AirMagnet WiFi Analyzer отслеживает процесс аутентификации клиента и определяет сигнатуры DoS-атак против точки доступа. Незавершенные транзакции аутентификации и подключения

запускают в приложении AirMagnet WiFi Analyzer процесс обнаружения атак и статистического сопоставления сигнатур. Обнаружение DoS-атаки приводят к подаче приложением AirMagnet WiFi Analyzer сигналов тревоги, которые включают подробное описание тревоги и информацию о целевом устройстве.

DoS-атака на клиентскую станцию

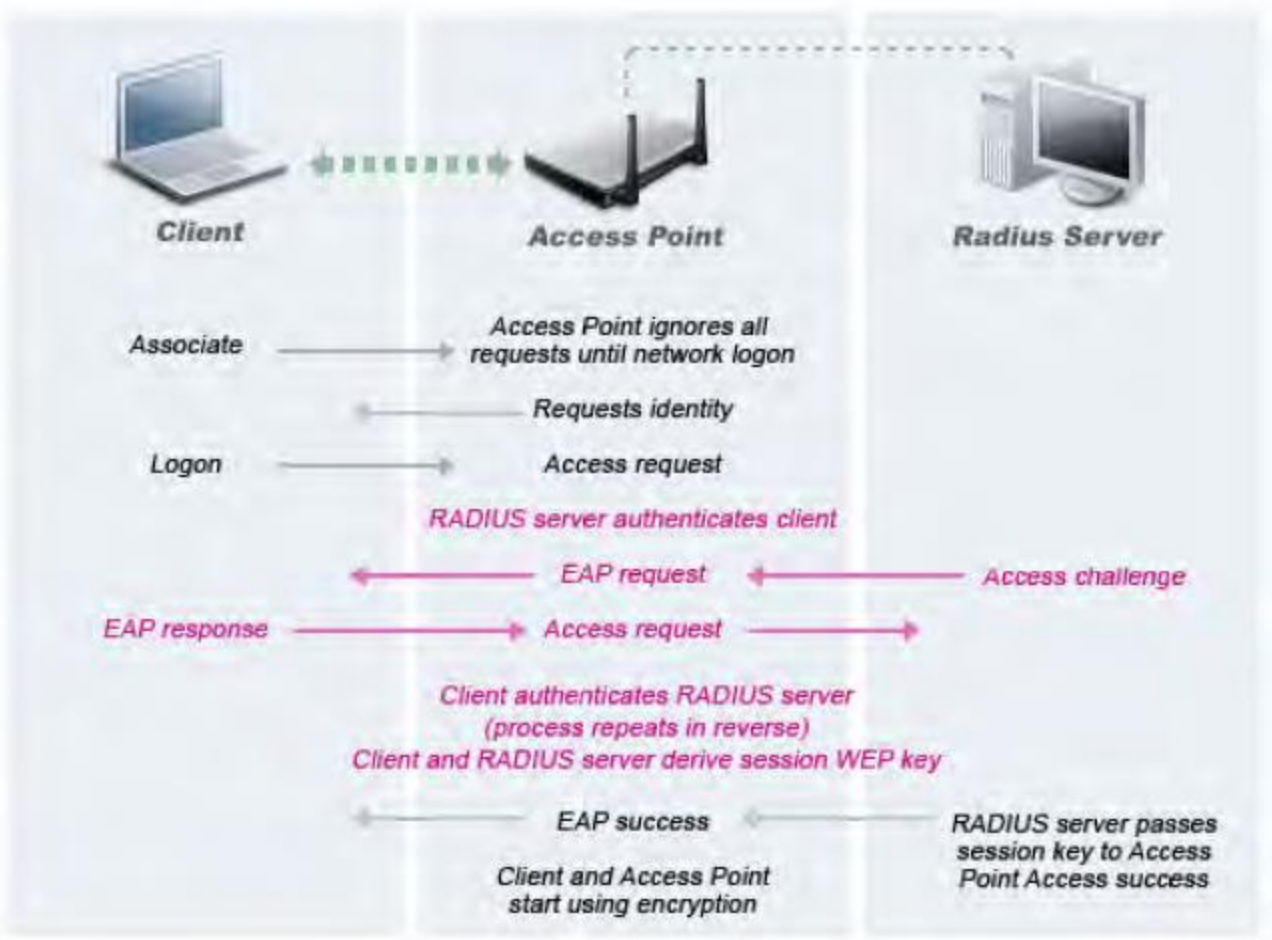
Атаки типа «отказ в обслуживании» против беспроводных клиентских станций обычно выполняются на основании того, что кадры управления 802.11 и протоколы аутентификации 802.1x не имеют механизма шифрования и, следовательно, могут быть подделаны. Например, злоумышленники могут нарушить обслуживание клиентской станции, непрерывно подменяя кадр разъединения или отмены аутентификации 802.11, передаваемый от точки доступа к клиентской станции. Ниже показана задаваемая стандартом IEEE машина состояний подключения 802.11, позволяющий проиллюстрировать то, как подключенную станцию можно обманом вывести из аутентифицированного и подключенного состояния с помощью различных типов фальшивых кадров.



State 1: …	Состояние 1: Аутентификация не пройдена, нет соединения
State 2:…	Состояние 2: Аутентификация пройдена, нет соединения
State 3:…	Состояние 3: Аутентификация пройдена, соединение установлено
Successful Authentication	Успешная аутентификация
Successful Authentication or Reassociation	Успешная аутентификация или повторное подключение
Deauthentication Notification	Извещение о деаутентификации
Diassociation Notification	Извещение о разъединении
Class 1…	Класс 1: Разрешенные кадры
Class 1 and 2…	Классы 1 и 2: Разрешенные кадры
Class 1, 2 and 3…	Классы 1, 2 и 3: Разрешенные кадры

Машина состояний подключения и аутентификации 802.11

Помимо атаки на состояние аутентификации и подключения 802.11 существуют аналогичные сценарии атак для аутентификации 802.1x. Например, сообщения 802.1x EAP-Failure или EAP-logoff не зашифровываются и могут быть подделаны для нарушения состояния аутентификации 802.1x, тем самым нарушая работу беспроводной сети. Для проверки подлинности 802.1x и изменения состояния обмена ключами смотрите приведенную ниже схему.



Client	Клиент
Access Point	Точка доступа
Radius Server	Сервер Radius
Associate	Подключение
Access Point ignores all requests…	Точка доступа игнорирует все запросы до входа в сеть
Requests Identity	Запрос идентичности
Logon	Вход
Access request	Запрос доступа
RADIUS server authenticates client	Сервер RADIUS аутентифицирует клиента
EAP request	Запрос EAP
Access challenge	Требование доступа
EAP response	Ответ EAP
Access request	Запрос доступа
Client authenticates RADIUS server…	Клиент аутентифицирует сервер RADIUS (процесс повторяется в обратном порядке). Клиент и сервер RADIUS создают ключ WEP для сеанса.
EAP success	Успешная аутентификация EAP
RADIUS server passes session key…	Сервер RADIUS передает ключ сеанса на точку доступа. Доступ выполнен успешно.
Client and Access Point…	Клиент и точка доступа начинают использовать шифрование

Процесс аутентификации пользователя 802.1x

Приложение AirMagnet WiFi Analyzer отслеживает процесс аутентификации клиента и определяет сигнатуры DoS-атак. Незавершенные транзакции аутентификации и подключения запускают в приложении AirMagnet WiFi Analyzer процесс обнаружения атак и статистического сопоставления сигнатур.

Обнаружение DoS-атаки приводят к подаче приложением AirMagnet WiFi Analyzer сигналов тревоги, которые включают подробное описание тревоги и информацию о целевом устройстве.

DoS-атака на инфраструктуру

Помимо атаки на точки доступа или клиентские станции злоумышленник может атаковать радиочастотный спектр или внутренний сервер аутентификации RADIUS с помощью атак типа «отказ в обслуживании». Радиочастотный спектр можно легко нарушить, внося на расстоянии радиочастотные шумы, создаваемые мощной антенной. Внутренние серверы RADIUS могут быть перегружены DDoS-атакой (распределенного отказа в обслуживании), когда несколько злоумышленников загружают сервер RADIUS запросами на аутентификацию. Эта атака даже не требует успешной аутентификации, а просто выполнения попыток аутентификации.

В этом разделе рассматриваются несколько различных атак:
- Атака флуда CTS
- Разработка Технологического университета Квинсленда
- Атака радиочастотных помех
- Атака виртуальной несущей

Ошибка конфигурации

Настроить и запустить сеть WLAN относительно легко, но гораздо сложнее поддерживать эффективную и надежную работу сетей WLAN среднего и крупного масштаба. Иногда проблемы с эффективностью и надежностью WLAN вызваны ошибками конфигурации. Для оптимизации производительности некоторыми из наиболее важных параметров конфигурации являются:
- Минимальная скорость передачи
- Длинная или короткая преамбула
- Функция PCF/DCF
- Порог RTS/CTS
- Порог фрагментации
- Максимальное количество повторов
- Несколько идентификаторов SSID
- Многое другое...

Приложение AirMagnet WiFi Analyzer контролирует и отслеживает использование этих параметров конфигурации. Сигналы тревоги подаются при обнаружении ошибок; например, когда идентификатор SSID, используемый устройствами в режиме инфраструктуры и устройствами в режиме ad-hoc, совпадает, чего никогда не должно быть в безопасной среде WLAN. Кроме того, несовместимые конфигурации устройств, использующих один и тот же идентификатор SSID, вызывают срабатывание тревоги в приложении AirMagnet WiFi Analyzer; например, находясь в пределах одного идентификатора SSID, одна точка доступа использует короткую радиочастотную преамбулу, а другая - длинную преамбулу. Это может вызвать проблемы для беспроводных станций, которые перемещаются между двумя точками доступа с разными конфигурациями и переключаются между ними. Приложение AirMagnet WiFi Analyzer обеспечивает последовательность и оптимальность конфигурации сети WLAN, уведомляя о любых проблемах с конфигурацией, а также предлагая оптимальную конфигурацию для использования.

Устройство не работает или неисправно

Нарушение работы беспроводной сети обычно происходит из-за отказа оборудования (сломанной антенны, сбоев электропитания или выхода из строя радиочастотного интерфейса точки доступа). Некоторые из этих проблем могут в конечном итоге исчезнуть сами по себе, не оставляя никаких следов для отслеживания основной причины до того момента, пока не повторятся снова. Другие же проблемы могут не исчезать самостоятельно, прерывая работу беспроводной сети на длительный период времени. Это одни из наиболее важных проблем, которые необходимо обнаруживать и устранять немедленно.

Приложение AirMagnet WiFi Analyzer способно обнаруживать такие проблемы, отслеживая радиочастотные сигналы и анализируя информацию, собранную поддерживаемыми AirMagnet картами WLAN. В дополнение к обнаружению каких-либо неработающих инфраструктурных устройств (обычно неработающей точки доступа) приложение AirMagnet Wi-Fi Analyzer также обнаруживает сброс прошивки

точки доступа и недостатки реализации функции управления энергосбережением 802.11, которые для некоторых беспроводных устройств являются широко известными проблемами.

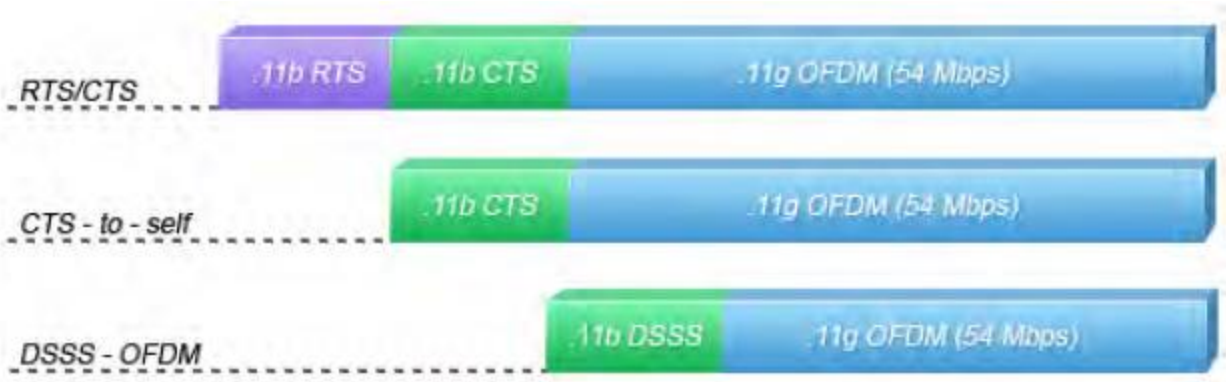
Проблемы с IEEE 802.11n и 802.11g

Проблемы с IEEE 802.11n

Буква «n» в обозначении спецификации 802.11 означает наличие множества новых функций и улучшений, позволяющих достичь максимальной пропускной способности не менее 100 Мбит/с. Как физический уровень (PHY), так и уровень управления доступом к среде (MAC) улучшены, что дает возможность достижения скорости передачи данных 600 Мбит/с. На физическом уровне (PHY) были представлены такие функции, как MIMO, пространственное разделение каналов, формирование луча передачи, пространственно-временное блочное кодирование, ширина канала 40 МГц и короткий защитный интервал; а эффективность на уровне доступа к среде (MAC) повышается с помощью таких методов, как объединение кадров и подтверждение блоков. Кроме того, указаны функции сосуществования, которые позволяют сети 802.11n быть обратно совместимой и сосуществовать с устаревшими системами (то есть сетями 802.11 a/b/g). Для подробного обсуждения функций протокола беспроводной сети 802.11n и их влияния на отрасль беспроводных локальных сетей, пожалуйста, обратитесь к техническому документу AirMagnet под названием «The Benefits and Challenges of 802.11n (Преимущества и проблемы 802.11n)», который размещен на веб-сайте AirMagnet по адресу https : //airmagnet.netally.com/my_airmagnet/.

Проблемы с IEEE 802.11g

Когда Институтом инженеров по электротехнике и радиоэлектронике (IEEE) был одобрен стандарт 802.11g, он вызвал большой интерес среди пользователей беспроводной связи. Уровень интереса был вторым по уровню после интереса, возникшего во время введения стандарта 802.11b. Стандарт 802.11g не только обеспечивает высокую скорость передачи данных, сопоставимую со стандартом 802.11a, но, что наиболее важно, обеспечивает обратную совместимость с широко применяемым стандартом 802.11b.



Mbps	Мбит/с

Стандарты IEEE 802.11 a/b/g и другие связанные спецификации уровня MAC

Подобно устройствам 802.11b, устройства 802.11g работают в диапазоне 2,4 ГГц Industrial Scientific Medical (ISM), но используют технологию ортогонального частотного разделения каналов (OFDM) для увеличения скорости и полосы пропускания (скорость передачи данных 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с). Также стандарт 802.11g поддерживает модуляцию кода Баркера и кодовой манипуляции (CCK), что обеспечивает скорости передачи данных 1, 2, 5,5 и 11 Мбит/с для обратной совместимости со стандартом 802.11b. Подобно стандарту 802.11b, устройства стандарта 802.11g ограничены тремя неперекрывающимися каналами, а новый физический уровень называется физическим уровнем с расширенной скоростью (ERP). Традиционно устройства 802.11b и 802.11g обмениваются данными с использованием схем модуляции CCK и OFDM, соответственно, но для обеспечения обратной совместимости устройства 802.11g должны поддерживать обе схемы модуляции.

Одобренный стандарт	801.11	801.11a	801.11b	801.11g
Доступная полоса частот	83,5 МГц	300 МГц	83,5 МГц	83,5 МГц
Нелицензируемые частоты	2,4 – 2,835 ГГц	5,150 – 5,250 ГГц (UNII-1)	2,4 – 2,835 ГГц	2,4 – 2,835 ГГц

		5,250 – 5,350 ГГц (UNII-2) 5,725 – 5,850 ГГц (UNII-3)		
Расширенный спектр	FHSS и DSSS	OFDM	DSSS	DSSS и OFDM
Неперекрывающиеся каналы	3 (в помещении и на улице)	4 (в помещении UNII-1) 4 (в помещении/на улице UNII-2) 4 (на улице UNII-3)	83,5 МГц	83,5 МГц
Каналы	FHSS – 78	36, 40, 44, 48 (UNII-1) 52, 56, 60, 64 (UNII-2) 149, 153, 157, 161 (UNII-3)	1 – 11 1, 6, 11 (неперекрывающиеся)	1 – 11 1, 6, 11 (неперекрывающиеся)
Скорость передачи данных на канал	2, 1 Мбит/с	54, 48, 36, 24, 18, 12, 9, 6 Мбит/с	11, 5ю5, 2, 1 Мбит/с	54, 36, 33, 24, 22, 12, 11, 9, 6, 5.5, 2, 1 Мбит/с
Тип модуляции	DQPSK: 2 Мбит/с DSSS DBPSK: 1 Мбит/с DSSS 4GFSK: 2 Мбит/с FHSS 2GFSK: 1 Мбит/с FHSS	BPSK: 6, 9 Мбит/с QPSK: 12, 18 Мбит/с 16-QAM: 24, 36 Мбит/с 64-QAM: 48, 54 Мбит/с	DQPSK/CCK: 11, 5.5 Мбит/с DQPSK: 1 Мбит/с	OFDM/CCK: 6, 9, 12, 18, 24, 36, 48, 54 Мбит/с OFDM: 6, 9, 12, 18, 24, 36, 48, 54 Мбит/с DQPSK/CCK: 33, 22, 11, 5.5 Мбит/с DQPSK: 1 Мбит/с DBPSK: 1 Мбит/с
Мощность: Северная Америка	1000 мВт 36 дБМ EIRP С использованием антенны 6 dBI	UNII-1: 40 мВт UNII-2: 200 мВт UNII-3: 300 мВт С использованием антенны 6 dBI	1000 мВт 36 дБМ EIRP С использованием антенны 6 dBI	1000 мВт 36 дБМ EIRP С использованием антенны 6 dBI
Мощность: Европа			100 мВт	
Мощность: Япония			100 мВт	

Диапазон и типы модуляции 802.11 a/b/g

Сеть WLAN, базирующаяся только на стандарте 802.11g (без устройств 802.11b), легко реализует дополнительную скорость и полосу пропускания, поддерживаемые стандартом 802.11g; однако ввод в сеть устройств 802.11b добавляет новый уровень сложности, связанный со смешанной средой b/g. В этом случае устройства 802.11g могут получить преимущество только за счет режима обратной совместимости, а эта функция стандартов 802.11g сопряжена со служебными данными. Недостаточно тщательное управление и настройка может легко привести не только к потере преимуществ 802.11g, но и к снижению производительности существующих устройств 802.11b. Для получения дополнительных сведений посетите веб-сайт AirMagnet (https://airmagnet.netally.com/my_airmagnet/), чтобы загрузить технический документ AirMagnet «802.11g – the need for speed».