Обнаружение несанкционированных точек доступа в Unified Wireless Networks

Содержание

Введение

Беспроводные сети расширяют границы проводных сетей и повышают производительность работников, упрощая доступ к информации. Однако несанкционированно развернутая беспроводная сеть привносит дополнительный риск с точки зрения безопасности. Защита порта в проводных сетях не является предметом особого внимания, а беспроводные сети организуются как простое расширение проводных сетей. Поэтому сотрудник, который приносит собственную точку доступа Cisco (AP) в хорошо защищенную беспроводную или проводную инфраструктуру и предоставляет доступ несанкционированным пользователям к сети, которая во всем остальном защищена, может легко поставить под угрозу безопасность сети.

Постороннее обнаружение позволяет администратору сети контролировать и устранять эту проблему безопасности. Архитектура Единой сети Cisco предоставляет два метода постороннего обнаружения, которые включают завершенную постороннюю идентификацию и решение для включения без потребности в дорогих и твердо выравниваемых по ширине оверлейных сетях и программных средствах.

Обзор функций

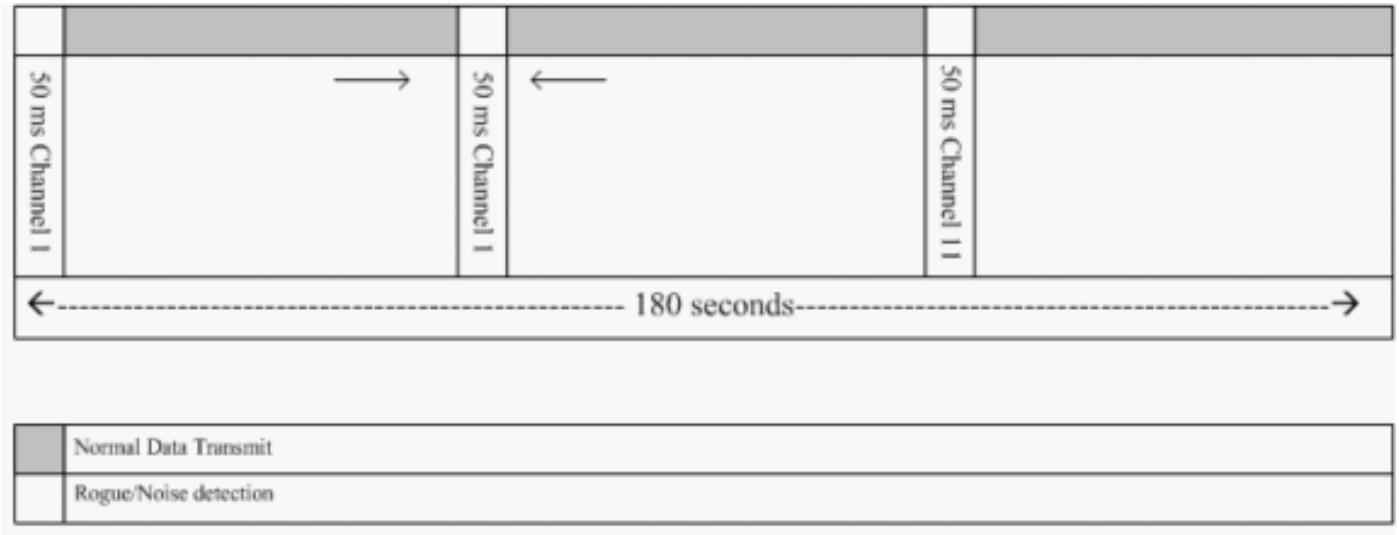
Постороннее обнаружение не связано никакими инструкциями, и никакое юридическое соблюдение не требуется для его операции. Однако постороннее включение обычно представляет юридические вопросы, которые могут поместить поставщика инфраструктуры в неудобную позицию, если оставлено для работы автоматически. Cisco чрезвычайно чувствительна к таким проблемам и предоставляет эти решения. Каждый контроллер настроен с Именем группы RF. Как только Легковесный AP регистрируется в контроллере, он встраивает **Элемент информации для аутентификации (IE)**, который является

определенным для RF Group, настроенной на контроллере во всех его ответных кадрах сигналов-маяков/зонда. Когда Легковесный AP слышит сигналы-маяки / тестовые ответные кадры от AP или без этого **IE** или с **неправильным IE**, тогда Легковесный AP сообщает, что AP, поскольку жулик, делает запись его BSSID в посторонней таблице и передает таблицу к контроллеру. Существует два метода, а именно, Посторонний протокол обнаружения местоположения (RLDP) и пассивная операция, которые объяснены подробно; посмотрите Определение Активного раздела Жуликов.

Обнаружение жулика инфраструктуры

Постороннее обнаружение в активной Беспроводной среде может быть дорогостоящим. Этот процесс просит, чтобы AP в обслуживании (или автономный режим) прекратил сервис, прислушался к шуму и выполнил постороннее обнаружение. Администратор сети настраивает каналы для сканирования и настраивает период времени, в котором просмотрены все станции. AP прислушивается к 50 мс для посторонних клиентских сигналов-маяков, затем возвращается к сконфигурированному каналу для обслуживания клиентов снова. Это активное сканирование, объединенное с соседними сообщениями, определяет, какие AP являются жуликами и какие AP допустимы и часть сети. Для настройки просмотренных каналов и периода времени сканирования, перейдите к **беспроводным сетям> 802.11b/g Сеть** (или **“b/g”** или в зависимости от требования к сети) и нажмите кнопку **Auto RF** в правом верхнем углу окна браузера.

Можно прокрутить вниз к **Шумовым/Интерференционным/Посторонним Каналам мониторинга** для настройки каналов, которые будут просмотрены для жуликов и шума. Доступные выборы: Все Каналы (1 - 14), Каналы Страны (1 - 11) или Ассоциация динамического канала (DCA) Каналы (по умолчанию 1, 6 и 11). Период времени сканирования через эти каналы может быть настроен в том же окне под **Интервалами Монитора (60 - 3600 secs)** наряду с интервалом измерения шума. По умолчанию интервал прослушивания для шума вне канала и жуликов составляет 180 секунд. Это означает, что каждый канал просматривается каждые 180 секунд. Это - пример каналов DCA, которые просматриваются каждые 180 секунд:



Как проиллюстрировано, большое число каналов, настроенных, чтобы быть просмотренным объединенный с короткими интервалами сканирования, оставляет меньше времени для AP фактически клиентам данных обслуживания.

Легковесный AP ждет для маркировки клиентов и AP как жулики, потому что об этих жуликах

возможно не сообщает другой AP, пока не завершен другой цикл. Тот же AP перемещается в тот же канал снова для мониторинга для посторонних AP и клиентов, а также шума и интерференции. Если те же клиенты и/или AP обнаружены, они перечислены как жулики на контроллере снова. Контроллер теперь начинает определять, привязаны ли эти жулики к локальной сети или просто к соседнему AP. В любом случае AP, который не является частью управляемой локальной беспроводной сети, считают жуликом.

Посторонние подробные данные

Легковесный AP идет вне канала для 50 мс для прислушиваний к посторонним клиентам, монитору для шума и интерференции канала. Любые обнаруженные посторонние клиенты или AP передаются контроллеру, который собирает эту информацию:

- Посторонний MAC-адрес AP
- Постороннее название AP
- Посторонний MAC-адрес подключенного клиента (клиентов)
- Защищены ли кадры с WPA или WEP
- Преамбула
- Отношение сигнала к шуму (SNR)
- Индикатор уровня сигнала получателя (RSSI)

Посторонняя точка доступа детектора

Можно заставить AP действовать в качестве постороннего детектора, который позволяет ему быть размещенным в магистральный порт так, чтобы это могло услышать, что вся проводная сторона подключила VLAN. Это продолжает находить клиента на проводной подсети на всех VLAN. Ложная точка доступа для обнаружения прислушивается к пакетам Протокола ARP для определения адресов Уровня 2 определенных посторонних клиентов или посторонних AP, передаваемых контроллером. Если адрес Уровня 2, которым соответствия найдены, контроллер, генерирует сигнал тревоги, который определяет посторонний AP или клиента как угроза. Этот сигнал тревоги указывает, что жулик был замечен на проводной сети.

Определите активные жулики

Посторонние AP должны быть “замечены” дважды, прежде чем они будут добавлены как жулик контроллером. Посторонние AP, как полагают, не являются угрозой, если они не связаны с проводным сегментом корпоративной сети. Чтобы определить, активен ли жулик, используются различные подходы. Те подходы включают RLDP.

Посторонний протокол обнаружения местоположения (RLDP)

RLDP является активным подходом, который используется, когда посторонний AP не имеет никакой аутентификации настроенная (Открытая аутентификация). Этот режим, который отключен по умолчанию, дает активному AP команду перемещаться в посторонний канал и подключение к жулику как клиент. В это время активный AP передает сообщения deauthentication всем подключенным клиентам и затем завершает работу радиоинтерфейса. Затем это свяжется к постороннему AP как клиент.

AP тогда пытается получить IP-адрес из постороннего AP и вперед пакета Протокола UDP

(порт 6352), который содержит локальный AP и постороннюю информацию о соединении к контроллеру через посторонний AP. Если контроллер получает этот пакет, будильник поставлен, чтобы уведомить администратора сети, что посторонний AP был обнаружен на проводной сети с функцией RLDP.

Примечание: Используйте **команду debug dot11 rldp enable**, чтобы проверить, привязывает ли Легковесный AP и получает адрес DHCP от постороннего AP. Эта команда также отображает пакет UDP, передаваемый Легковесным AP контроллеру.

Выборку UDP (порт назначения 6352) пакет, переданный Легковесным AP, показывают здесь:

```
0020 0a 01 01 0d 0a 01 .......(.*...... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00
......x......... 0040 00 00 00 00 00 00 00 00 00 00
```

Первые 5 байтов данных содержат адрес DHCP, данный точке доступа в локальном режиме посторонним AP. Следующими 5 байтами является IP-адрес контроллера, придерживавшегося на 6 байтов, которые представляют посторонний MAC-адрес AP. Затем существует 18 байтов нулей.

Пассивная операция:

Когда посторонний AP имеет некоторую форму проверки подлинности, или WEP или WPA, этот подход используется. Когда форма проверки подлинности настроена на постороннем AP, Легковесный AP не может связаться, потому что это не знает ключ, настроенный на постороннем AP. Процесс начинается с контроллера, когда это передает список посторонних MAC - адресов клиента к AP, который настроен как посторонний детектор. Посторонний детектор просматривает все связанные и настроенные подсети для запросов ARP, и ARP ищет соответствующий адрес Уровня 2. Если соответствие обнаружено, контроллер уведомляет администратора сети, что жулик обнаружен на проводной подсети.

Активное постороннее включение

Как только посторонний клиент обнаружен на проводной сети, администратор сети в состоянии содержать и посторонний AP и посторонних клиентов. Это может быть достигнуто, потому что de-пакеты-проверки-подлинности 802.11 передаются клиентам, которые привязаны к посторонним AP так, чтобы была смягчена угроза, что такая дыра создает. Каждый раз существует попытка содержать посторонний AP, почти 15% ресурса Легковесного AP используются. Поэтому предложено физически определить местоположение и удалить посторонний AP, как только это содержится.

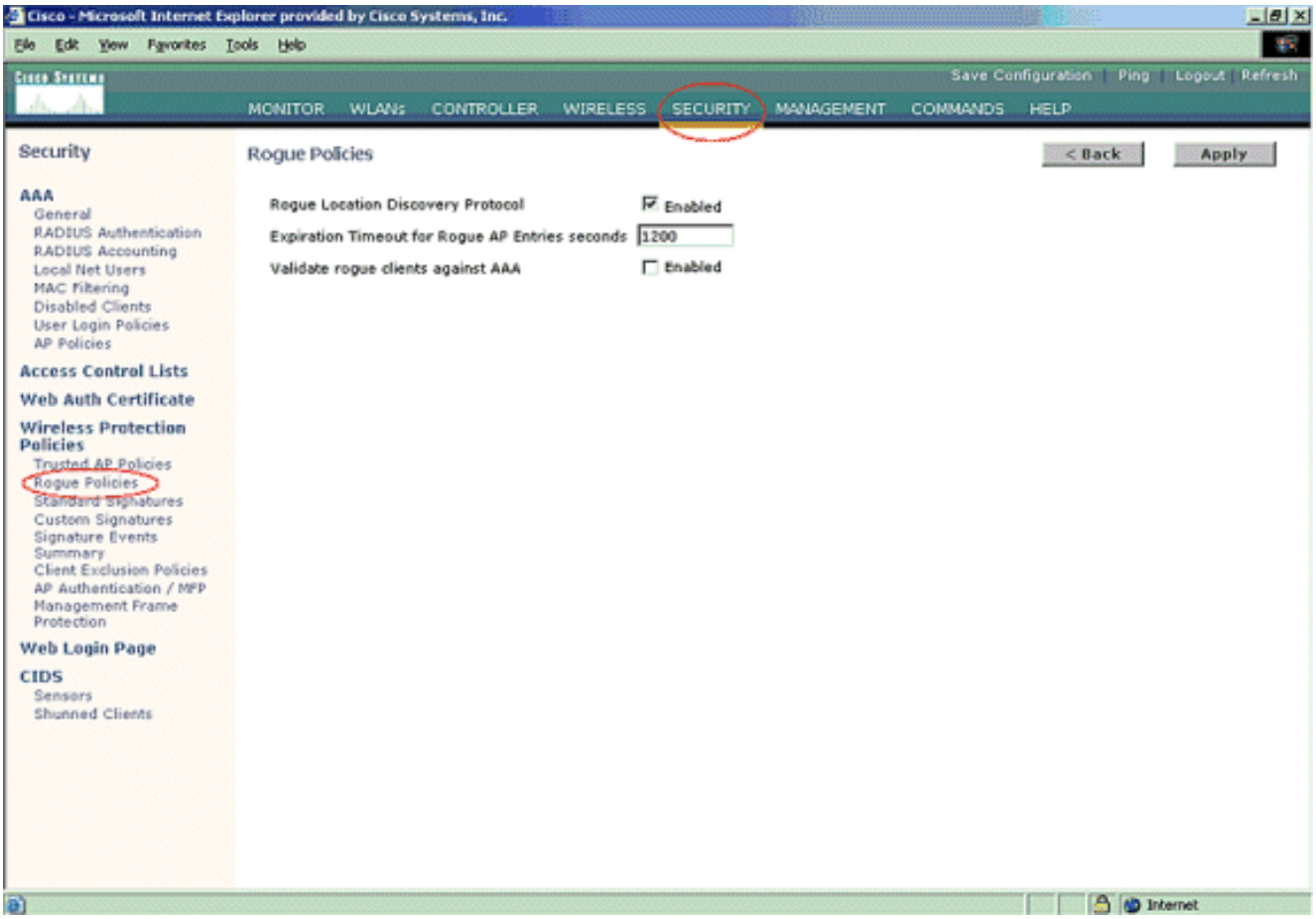
Примечание: От выпуска 5.2.157.0 WLC, когда-то помада обнаружена, можно теперь принять решение или вручную или автоматически содержать обнаруженный жулик. В выпусках ПО контроллера до 5.2.157.0, ручное включение является единственной опцией.

Постороннее обнаружение – действия настройки

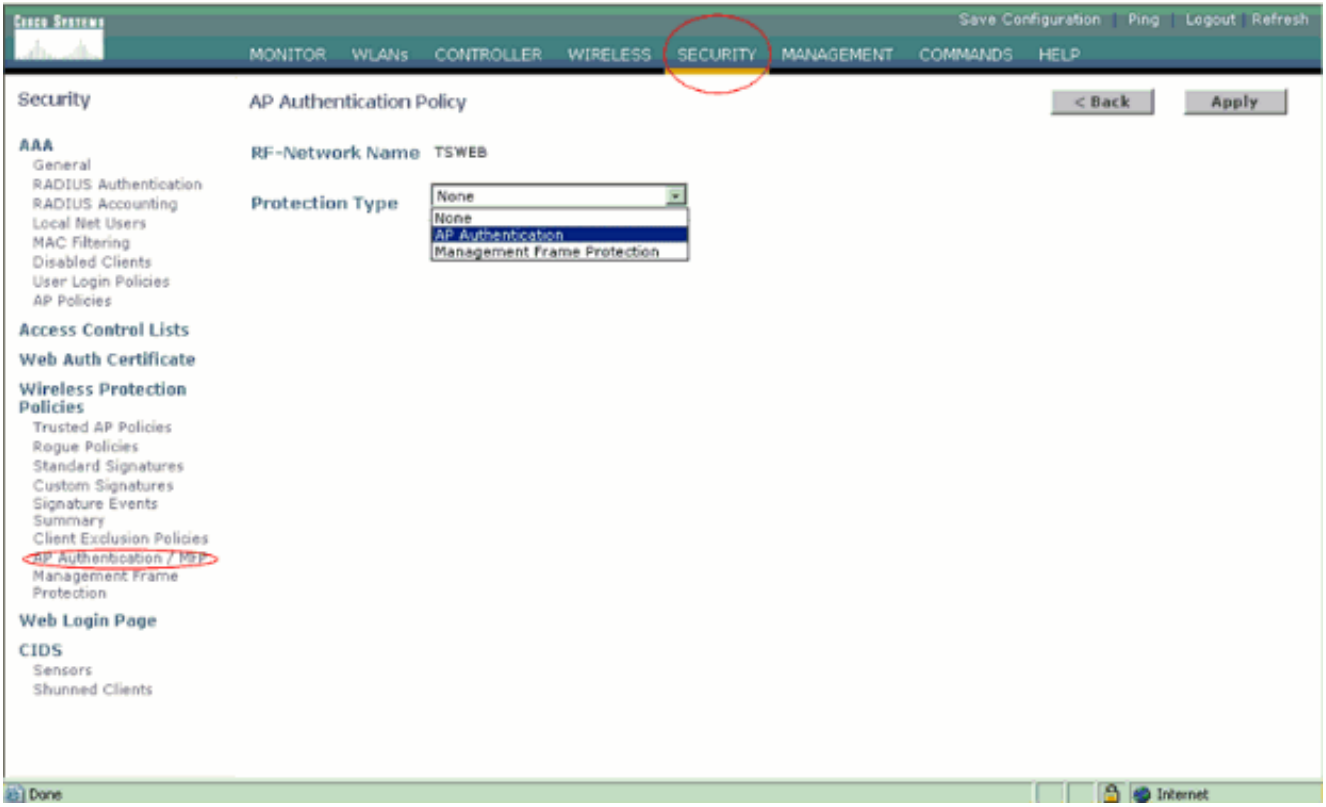
Почти вся посторонняя конфигурация обнаружения позволена по умолчанию обеспечить увеличенный, out-of-the-box сетевая безопасность. Эти действия настройки предполагают, что никакое постороннее обнаружение не установлено на контроллере для разъяснения важной посторонней информации об обнаружении.

Для устанавливания постороннего обнаружения выполните эти шаги:

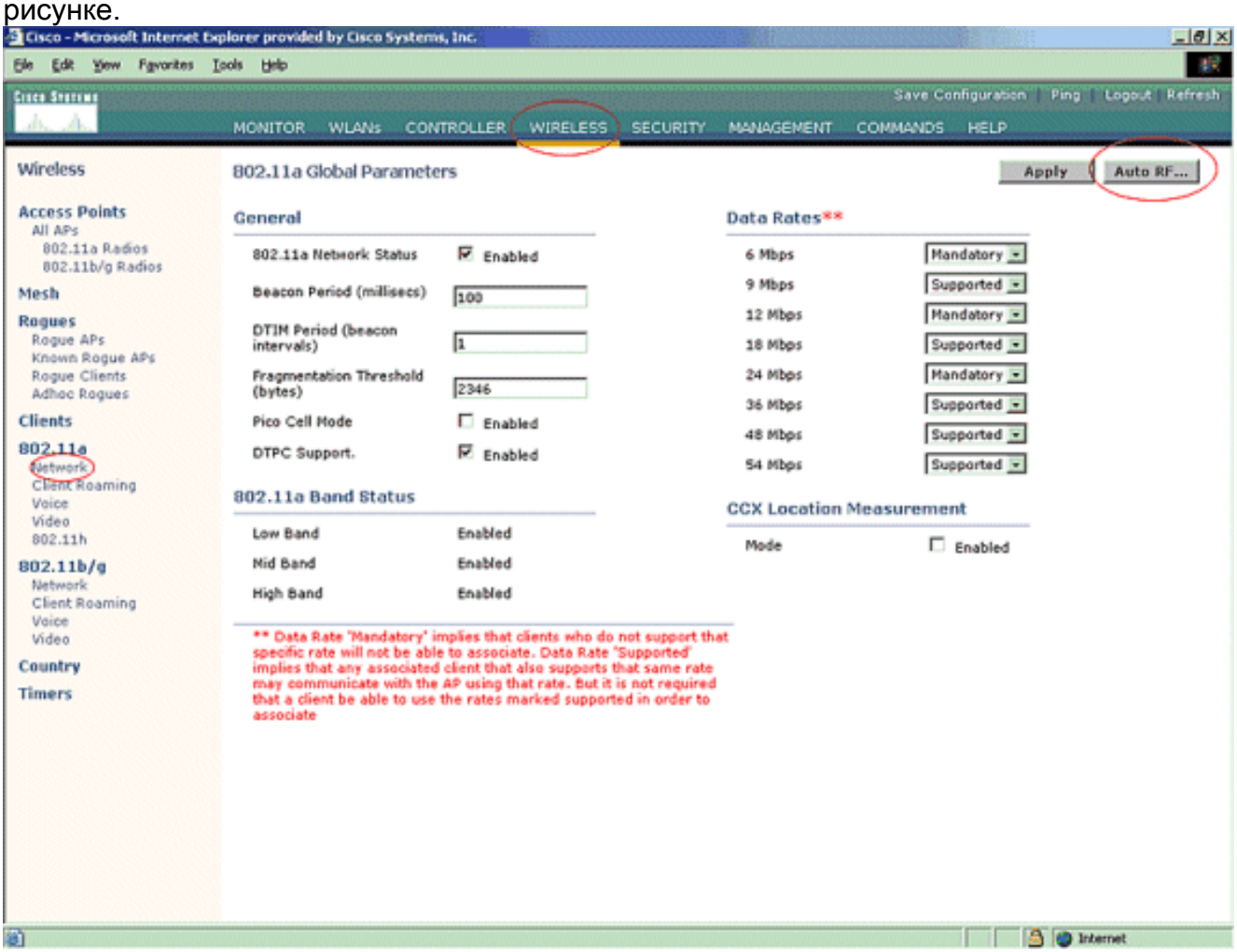
1. Гарантируйте, что включен Посторонний Протокол обнаружения Местоположения. Для включения его выберите **Security> Rogue Policies** и нажмите **Enabled** на **Постороннем Протоколе обнаружения Местоположения** как показано на рисунке.**Примечание:** Если посторонний AP не слышат для определенной величины времени, он удален, формируют контроллер. Это - **Таймаут Истечения** для постороннего AP, который настроен ниже опции
RLDP.



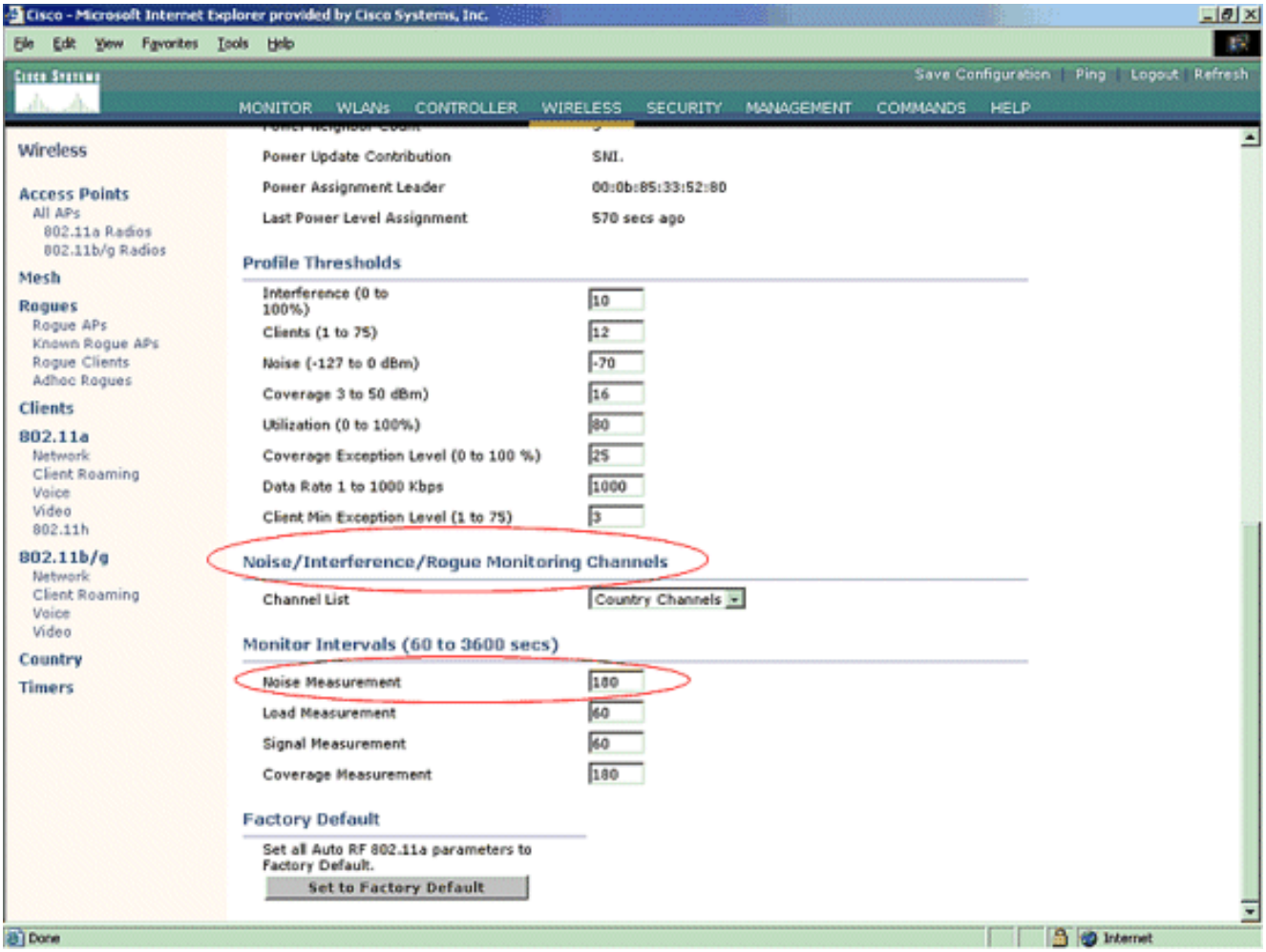
2. Это - необязательное действие. Когда эта опция активирована, о AP, передающих пакеты соседнего узла RRM с другими **Именами групп RF**, сообщают как жулики. Это будет полезно в изучении вашей среды RF. Для включения его выберите **Security-> AP Authentication**. Затем выберите **AP Authentication** в качестве Типа защиты как показано на
рисунке.



3. Проверьте каналы, которые будут просмотрены в этих шагах:Выберите **Wireless> 802.11a Сеть**, тогда **Автоматический RF** в правой стороне как показано на рисунке.



На странице **Auto RF** прокрутите вниз и выберите **Noise/Interference/Rogue Monitoring Channels**.



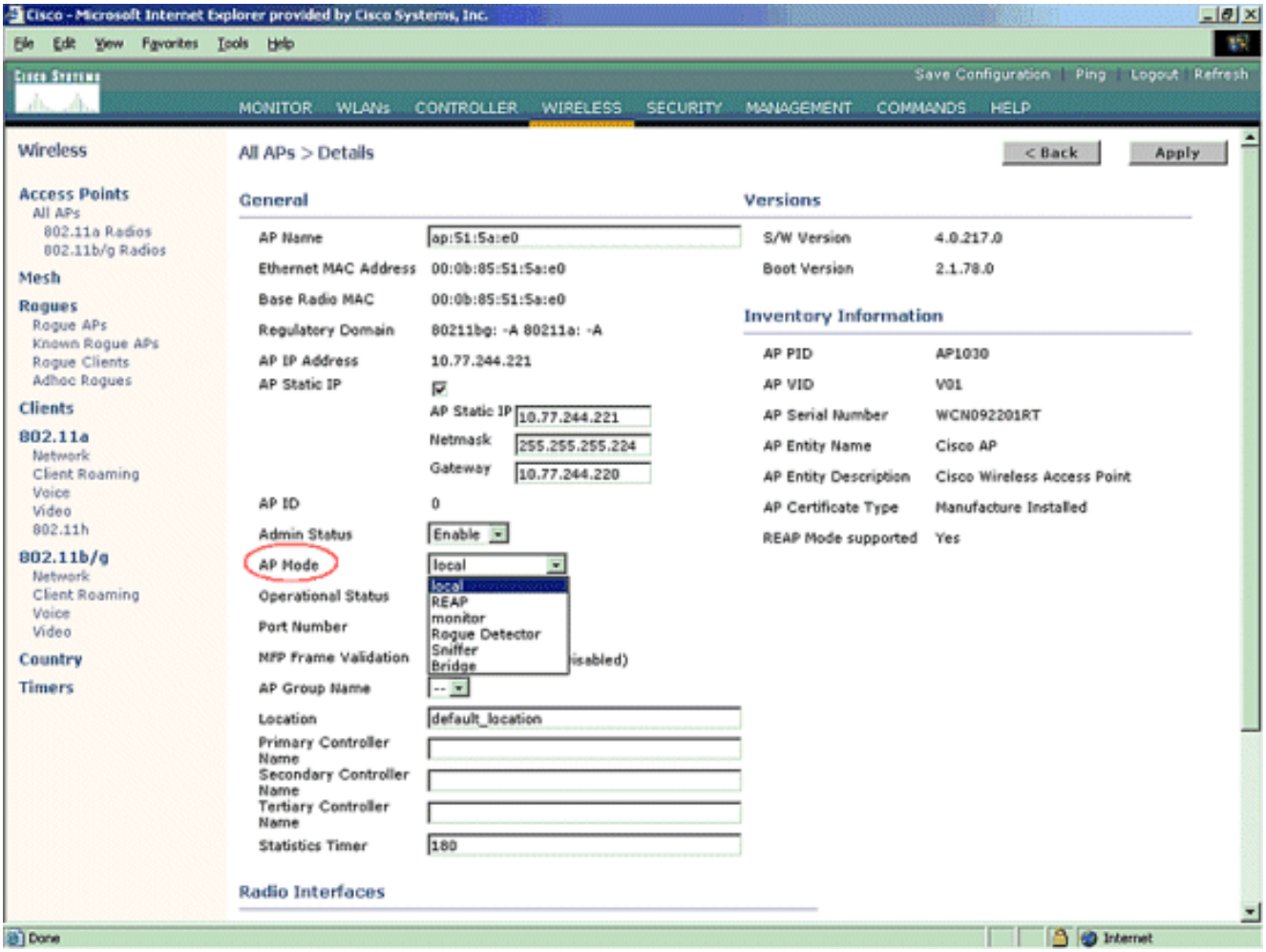
Список Канала детализирует каналы, которые будут просмотрены для постороннего мониторинга, в дополнение к другому контроллеру и функциям AP. См. часто задаваемые вопросы Облегченной точки доступа для получения дополнительной информации о Легковесных AP и часто задаваемые вопросы Устранения неполадок Контроллера беспроводной локальной сети (WLC) для получения дополнительной информации о контроллерах беспроводной локальной сети.

Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

4. Установите Период времени для сканирования выбранных каналов:Продолжительность сканирования определенной группы каналов настроена под **Интервалами Монитора> Измерение шума**, и допустимый диапазон с 60 до 3600 секунд. Если оставлено в по умолчанию 180 секунд, AP просматривают каждый канал в группе каналов однажды, для 50 мс, каждые 180 секунд. В течение этого периода, изменений радио AP от его канала обслуживания до указанного канала, слушает и делает запись значений сроком на 50 мс, и затем возвращается к исходному каналу.

Время перехода плюс жить время 50 мс берет AP, вне канала приблизительно для 60 мс каждый раз. Это означает, что каждый AP тратит приблизительно 840 мс из общих 180 секунд, прислушиваясь к жуликам.“Слушание” или “живет”, время не может модифицироваться и не изменено с корректировкой значения Измерения шума. Если таймер Измерения шума будет понижен, то посторонний процесс обнаружения, вероятно, найдет больше жуликов и найти их более быстро. Однако это улучшение прибывает за счет целостности данных и сервиса клиента. Более высокое значение, с другой стороны, обеспечивает лучшую целостность данных, но понижает способность найти жулики быстро.

5. Настройте Режим AP операции:Легковесный Режим AP операции определяет роль AP. Режимы, отнесенные к информации, содержащейся в данном документе:**Локальный** — Это - нормальная работа AP. В то время как сконфигурированные каналы просмотрены для шума и жуликов, этот режим позволяет клиентам данных обслуживаться. В этом режиме работы AP идет вне канала для 50 мс и прислушивается к жуликам. Это циклически повторяется через каждый канал, по одному, в течение периода, заданного под Автоматической конфигурацией RF.**Монитор** — Это - радио, получают только режим, и позволяет AP просматривать все сконфигурированные каналы каждые 12 секунд. Только de-пакеты-проверки-подлинности передаются в воздухе с AP, настроил этот путь. Точка доступа в режиме мониторинга может обнаружить жулики, но она не может соединиться с подозрительным жуликом как клиент для передачи пакетов RLDP.**Примечание:** DCA обращается к не-Перекрытым каналам, которые конфигурируемы с режимами по умолчанию.**Посторонний Детектор** — В этом режиме, радио AP выключено, и AP слушает проводной трафик только. Контроллер передает AP, настроенные как посторонние детекторы, а также списки подозреваемых посторонних клиентов и MAC-адресов AP. Посторонний детектор прислушивается к пакетам ARP только и может быть связан со всеми широковещательными доменами через магистральную линию при желании.Можно настроить отдельный Режим AP просто, как только Легковесный AP связан с контроллером. Для изменения Режима AP соединитесь с веб-интерфейсом контроллера и перейдите к **беспроводным сетям**. Щелкните **по Details** рядом с желаемым AP к тому, для отображения экрана, подобного этому:



Используйте раскрывающееся меню Режима AP для выбора желаемого Режима AP операции.

Команды для устранения неполадок

Можно также использовать эти команды для устранения проблем конфигурации на AP:

- **show rogue ap summary** — Эта команда отображает список посторонних AP, обнаруженных Легковесными AP.
- **show rogue ap detailed** *<MAC-адрес постороннего AP>* — Использование эта команда, чтобы посмотреть детали об отдельном постороннем AP. Это - команда, которая помогает определять, включен ли посторонний AP на проводную сеть.

Заключение

Постороннее обнаружение и включение в централизованном решении для контроллера Cisco являются самым эффективным и наименее навязчивым методом в отрасли. Гибкость, предоставленная администратору сети, обеспечивает более специализированную адаптацию, которая может принять любые требования к сети.

Дополнительные сведения

- Обзор RF Groups

- Cisco Systems – техническая поддержка и документация