Cisco Aironet Access Point FAQ

Содержание

Введение

Этот документ предоставляет ответы на большинство часто задаваемых вопросов (FAQ) о точках доступа Cisco Aironet (AP).

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Вопросы проектирования

Вопрос. . Каковы имя пользователя по умолчанию и пароль для Cisco IOS® Software-based APs?

О. AP на основе ПО Cisco IOS имеют конфигурацию по умолчанию, которая включает комбинацию имени пользователя и пароля, обоими из которых является (чувствительная к регистру) **Cisco**. После сброса точки доступа к заводским параметрам по умолчанию будьте готовы ввести слово "Cisco" в поля имени пользователя и пароля, когда графический интерфейс или интерфейс командной строки (CLI) предложит сделать это.

Вопрос. . Какой кабель я должен использовать для консольного соединения?

О. Используйте прямой кабель с девятиконтактным штекером к девятиконтактным розеткам разъема для соединения COM1 или порта COM2 на компьютере к порту RS-232 на AP. На компьютере необходимо запустить программу эмуляции терминала, например:

- Microsoft Windows HyperTerminal
- Symantec ProComm
- Минисом

Используйте следующие параметры портов:

Скорость:	9600 бит в секунду (бит/с)
Количество информационных битов:	8

Стоповые биты:	1
Паритет:	Нет
Управление потоком данных:	Xon/Xoff

Примечание: Если Xon/Xoff управления потоками не работает, попытайтесь использовать управление потоками Ни один.

Вопрос. . У меня есть AP Aironet 1231 года. Производит ли Cisco кабель расширения длиной 50 футов, который позволяет устанавливать точку доступа и антенну в разных помещениях?

О. Да, номер изделия 50-футового кабеля является AIR-CAB050LL-R. Можно использовать этот кабель для соединения AP с антенной.

Вопрос. . Как вы проверяете радио-тип на автономном AP?

О. Можно использовать **команду show controllers** от привилегированного режима EXEC на AP для получения информации о радио-типе.

Вопрос. . Как вы устанавливаете IP-адрес на AP?

О. По умолчанию AP запрашивает IP-адрес через DHCP.

Cisco IOS Release 12.3 (2) JA и более позднее изменение поведение по умолчанию AP, запрашивающих IP-адрес от сервера DHCP:

- При соединении AP серии 1230 или 1200 года с конфигурацией по умолчанию к LAN AP запрашивает IP-адрес от сервера DHCP. Если это не получает адрес, это продолжает отправлять запросы неопределенно.
- При соединении AP серии 1100 с конфигурацией по умолчанию к LAN AP серии 1100 предпринимает несколько попыток получить IP-адрес от сервера DHCP. Если это не получает адрес, это назначает себя IP-адрес 10.0.0.1 в течение пяти минут. Во время этого пятиминутного окна можно перейти к IP - адресу по умолчанию и настроить статический адрес. Если после пяти минут AP не реконфигурирован, он сбрасывает от этих 10.0.0.1 адресов и возвращается к запросу адреса от сервера DHCP. Если это не получает адрес, это отправляет запросы неопределенно. При пропавших без вести пятиминутного окна для просмотра к AP в 10.0.0.1 можно выключить AP для повторения процесса.

Можно также вручную установить IP-адрес AP. На компьютере под управлением Microsoft Windows, подключенном к сегменту Ethernet, из командной строки DOS выполните следующую команду:

```
arp -s a.b.c.d 00-12-34-56-78-90
```

Примечание: Условие *a.b. c . d* представляет IP-адрес, который должен быть установлен на AP, и *00-12-34-56-78-90* MAC-адрес. Этот адрес можно найти на панели в нижней части точки доступа.

Для проверки адреса используется следующая команда:

```
ping a.b.c.d
```
Примечание: Если AP уже назначил IP-адрес другой метод, эта процедура не работает.

Вопрос. . Как вы включаете доступ HTTPS на AP?

O. Для включения HTTPS необходимо добавить эту команду к AP:

```
AP(config)#ip http secure-server
```
Когда вы добавляете **команду ip http secure-server**, вы видите ключи RSA, требуемые для безопасной связи, восстановленной на AP.

Вопрос. . Как клиент выбирает точку доступа (AP), которая будет привязана?

O. Выбор точки доступа (AP) сделан по радио машины клиента. На основе изготовителя, драйвера, типа карты, и т.д, это может использовать другие метрики, чтобы сделать выбор. Самый простой механизм присоединения точек доступа, используемый в большинстве клиентов, основывается на уровне сигнала, который клиент получает от точки доступа. Стандарт 802.11 требует только, чтобы клиентская беспроводная карта сообщила об уровне сигнала с простой метрикой, названной индикатором мощности принимаемого сигнала (RSSI). После этого клиент присоединяется к точке доступа с наибольшим уровнем сигнала. Хорошо известно, что подобные алгоритмы могут привести к ухудшению производительности. Главная причина — отсутствие информации о загрузке различных точек доступа.

Вопрос. . Беспроводной клиент может переместиться между AP LWAPP и автономными AP?

O. Нет, роуминг между LAP и автономными AP НЕ поддерживается. Причина состоит в том, что, когда связано с AP LWAPP, трафик передают через туннель LWAPP. С тех пор нет никакого туннеля мобильности между Контроллером беспроводной локальной сети и автономными AP, перемещение не работает.

Вопрос. . Как вы расширяете покрытие AP?

O. Существует несколько способов расширить зону уверенного приема для AP. Это самые важные методы:

- Использование точек доступа в режиме повторителя.
- Использование вторичной точки доступа в режиме точки доступа на канале, который не накладывается на канал первичной точки доступа.
- Измените параметр уровня мощности передатчика существующего AP для расширения покрытия.
- Установка точек доступа в оптимальном положении.

Полное описание внедрения этих методов см. в документе Методы расширения зоны действия радиомодулей в сетях WLAN.

Вопрос. . Если ваш AP находится в режиме повторителя, каковы результаты?

O. В режиме репитера Ethernet-порт отключен. Полезная пропускная способность

уменьшается на половину при каждом переходе от родительской точки доступа.

Для устанавливания повторителей необходимо включить Расширения Aironet и на родительской (корневой) точке доступа и на точках доступа повторителя. Расширения Aironet, которые включены по умолчанию, улучшают способность точки доступа понять возможности устройств клиента Cisco Aironet, привязанных к точке доступа. При отключении Расширений Aironet можно иногда улучшать совместимость между устройствами клиента не-Cisco и точкой доступа. Устройства клиента не-Cisco могут найти связь трудной с точками доступа повторителя и точкой доступа к корневому каталогу, к которой привязаны повторители.

SSID инфраструктуры должен быть назначен на собственный VLAN. Если несколько VLAN созданы на точке доступа или беспроводном мосту, SSID инфраструктуры не может быть назначен на несобственный VLAN. Когда SSID инфраструктуры настроен на несобственном VLAN, это сообщение появляется:

```
SSID [xxx] must be configured as native-vlan before enabling
 infrastructure-ssid
```

Поскольку точки доступа создают виртуальный интерфейс для каждого радиоинтерфейса, партнер точек доступа повторителя к доступу к корневому каталогу указывают дважды: однажды для фактического интерфейса и однажды для виртуального интерфейса.

Примечание: Вы не можете настроить несколько интерфейсов VLAN на точках доступа повторителя. Точки доступа повторителя поддерживают только собственный VLAN.

Вопрос. . Что функции поддерживаются опцией Aironet Extension?

О. Расширение Aironet является специальным средством, внедренным Cisco. Расширения Aironet содержат информационные элементы, которые поддерживают эти функции.

- **Распределение нагрузки:** Точка доступа использует Расширения Aironet для прямых устройств клиента к точке доступа, которая предоставляет лучшее соединение с сетевым на факторах, таких как количество пользователей, уровней ошибок в канале связи, загрузки и уровня сигнала.Распределение нагрузки является составляющим собственность между устройствами, которые понимают Расширения Aironet. Распределение нагрузки внедрено расширениями в сигналах-маяках AP и/или тестовых ответах, которые предоставляют сведения о них:Уровень сигнала базовой станцииЗагрузка базовой станции (занятый передатчик %)Количество переходов до мозга костейКоличество связываний клиентаКлиент оценивает их и связывается к "лучшему". Клиенты не-Cisco не понимают эти расширения.
- **MIC:** Cisco Составляющий собственность Message Integrity Check (MIC) — MIC является дополнительной характеристикой безопасности WEP, которая предотвращает атаки на зашифрованные пакеты, названные разрядно-зеркально отраженными атаками. MIC внедрен и на точке доступа и на всех связанных устройствах клиента.
- **Составляющий собственность Протокол временной целостности ключа Cisco (CKIP)**, также известный как Хэширование ключа WEP, является дополнительной характеристикой безопасности WEP, которая защищает от атаки на WEP, в котором злоумышленник использует незашифрованный сегмент, названный Вектором инициализации (IV) в зашифрованных пакетах для вычисления Ключа WEP.
- В дополнение к ним Расширения Aironet несут дополнительные сведения, которые

включают их:Загрузка, которую в настоящее время обрабатывает APКоличество переходов от Проводной сетиТип устройства, который помогает определять продукт под системой Cisco для управленияDevice NameКоличество связанных клиентовРадио-тип, функция использовала определять определенные характеристики о радио, такие как скорость передачи данных, радио-тип (1310, 1200, 352 или 342), тип безопасности (WEP/802.1x), и т.д.

Устройства, которые являются CCX, совместимым также, могут использовать преимущества некоторых функций Расширения Aironet. Вот список функций, доступных с другими версиями Cisco Compatible Extensions:

Cisco Compatible Extensions - версии и функции

Вопрос. . Можно ли подключить два компьютера вместе без AP через карты беспроводного интерфейса?

O. Да. В приложении Aironet Client Utility (ACU) можно настроить клиенты на работу в режиме ad hoc. Это подключение может быть только одноранговым. Один из компьютеров становится родительским и управляет подключением. Другие компьютеры режиме ad hoc становятся дочерними станциями.

Вопрос. . Требуется ли специальное оборудование для поддержки шифрования?

O. Конкретная модель оборудования определяет уровень шифрования для блока:

- 341 и 351 модель только поддерживает 40-разрядное шифрование.
- Модели 342 и 352 поддерживают как 40-битное, так и 128-битное шифрование.
- Все модели серии 1100, 1200 и 1300 поддерживают 40-битное и 128-битное шифрование.

Вопрос. . Действительно ли возможно просмотреть все AP и их связанных клиентов, которые принадлежат той индивидуальной сети / инфраструктура только от одиночного AP?

O. Это возможно от AP VxWorks. Одна точка доступа VxWorks может отображать информацию обо всех клиентах и точках доступа в сети. Это может быть достигнуто при нажатии **Association> Entire Network> Apply**. Если образ в AP является образом LWAPP, в на основе IOS AP, это не отображает всех связанных клиентов в той сети без справки устройства управления, таких как WLSE, с одним AP как WDS или контроллер.

Вопрос. . Я использую CCKM в своей сети, но тем не менее весь процесс проверки подлинности происходит каждый раз, когда перемещается устройство клиента. Т. е. функции быстрого и безопасного роуминга не работают. В чем причина?

O. Это - возможно из-за дефекта CSCsg10128. Эта ошибка исправлена в версии 3.1.03.

Вопрос. . Если существует повреждение кабеля Уровня 1/уровня 2, точки

доступа Cisco поддерживают функцию Протокола UDLD для завершения работу Подключения по технологии Ethernet к коммутаторам?

O. Нет, точки доступа Cisco не поддерживают функцию UDLD.

Вопрос. . Как вы подаете питание к AP Aironet?

O. Электропитание для вашего AP зависит от использованной модели точки доступа, которую вы имеете. Дополнительные сведения см. в документе Варианты питания для точек доступа Cisco Aironet и контроллеров WLC.

Вопрос. . У меня есть AP1010, AP1030 и AIR-LAP-1232AG. Могут ли они использовать модуль WS-PWR-PANEL для питания через Ethernet (PoE)?

O. WS-PWR-PANEL только поддерживает точки доступа с одиночным радио. См. матрицу совместимости, доступную в *PoE Cisco и* разделе *Cisco Intelligent Power Management* Питания Cisco Aironet Над Примечанием к приложению Ethernet для получения дополнительной информации.

Вопрос. . Как вы сохраняете конфигурацию AP?

O. Модификации к конфигурации сразу сохранены. **Конфигурацию можно сбросить в текстовый формат из меню Setup. Затем выберите Cisco Services (Службы Cisco) > Manage System Configuration (Управление конфигурацией системы) и загрузите системную конфигурацию.**

Вопрос. . Как я определяю определенную частоту или канал, что мой AP или соединяет использование?

O. Используйте **команду show controllers dot11Radio0**, чтобы показать частоту и канал, что идут AP или мост. В примере выходных данных ниже показано, как найти эти сведения:

```
ap#show controllers dot11Radio0 ! interface Dot11Radio0 Radio AIR-AP1242GA, Base Address
0014.1b58.08f Version 5.80.12 Serial number: GAM09200992 Number of supported simultaneous BSSID
on Dot1 Carrier Set: Americas (US ) DFS Required: No Current Frequency: 2412 MHzChannel 1
```

Вопрос. . Как я заставляю свой AP работать с другими устройствами IEEE 802.11b?

O. Чтобы позволить AP связаться с другим 802.11b устройство, выключите Расширения Aironet. **Установите флажок Non-Aironet 802.11 в окне "Express Setup". Другой способ: щелкните переключатель Use Aironet Extension в окне "Advanced AP Radio".**

Вопрос. . Какие устройства могут связаться с AP?

- Точка доступа — клиент
- Точка доступа — точка доступа (в режиме повторителя)
- Точка доступа (в режиме повторителя) — базовая станция (в режиме точки доступа)
- Точка доступа — мост рабочей группы

Вопрос. . В какой частоте связывается AP?

O. В Соединенных Штатах AP IEEE 802.11b передают и получают в одном из 11 каналов в 2.4 Частотах ГГц. Точки доступа IEEE 802.11a передают и принимают данные на одном из 8 каналов на частоте 5 ГГц. Точки доступа IEEE 802.11g передают и принимают данные на одном из 11 каналов на частоте 2,4 ГГц. Это общедоступные диапазоны частот, которые не лицензируются FCC.

Вопрос. . Как вы защищаете данные через ссылку радио AP?

O. Существует несколько методов для обеспечения данных через беспроводное соединение AP. Дополнительные сведения о различных методах обеспечения безопасности см. в документе Вопросы и ответы по безопасности Cisco Aironet.

Вопрос. . Сколько клиентов может связаться к AP?

O. AP имеет физическую емкость для обработки 2048 MAC-адресов, но, потому что AP является общими средствами связи и действует как беспроволочный концентратор, производительность каждого пользователя уменьшения как количество пользовательских увеличений на отдельном AP. Идеально, не больше чем 24 клиента могут связаться с AP, потому что пропускная способность AP уменьшена с каждым клиентом, который связывается к AP.

Вопрос. . Существует ли ограничение на количество Фильтров MAC - адресов, которые могут быть настроены на AP?

O. Можно использовать CLI для настройки до 2,048 MAC-адресов для фильтрации, но с использованием интерфейса веба - обозревателя можно настроить только до 43 MAC-адресов для фильтрации.

Вопрос. . Каков типичный диапазон для AP?

O. Ответ на этот вопрос зависит от многих факторов, которые включают их:

- Скорость передачи данных (пропускная способность), которой вы желаете
- Тип антенны
- Длина кабеля антенны
- Устройство-приемник

В оптимальной установке диапазон может быть до 300 футов.

Вопрос. . Каковы доступные параметры настройки уровня мощности передачи для AP 1200 года?

O. Параметры настройки мощности передачи являются другими и зависят по радио, которое используется. См. Таблицу данных точки доступа Cisco Aironet серии 1200 для полного списка уровней значения питания. Поскольку параметры мощности зависят от канала, выполните обследование узла. Обследование узла очень важно для получения точной информации о том, какой параметр необходимо использовать. Дополнительные сведения об обследовании см. в документе Вопросы и ответы по обследованию

беспроводного узла.

Вопрос. . Как я могу установить AP так, чтобы только могли соединиться клиенты IEEE 802.11g? Я не хочу, чтобы клиенты IEEE 802.11b подключались к точке доступа и замедляли беспроводную сеть. Для небезопасных клиентов существует вторая, параллельная сеть 802.11b.

O. Для AP для получения только клиентов 802.11g выполните эти шаги в GUI:

1. **Перейдите к разделу "Network Interfaces" и щелкните Radio 0-802.11G.**
2. **Выберите вкладку Settings в верхней части окна "Radio 0-802.11G".**
3. **Выберите Disable для следующих скоростей передачи данных:** 1.02.05.511.0
4. **Выберите Require для всех остальных скоростей передачи данных.** Это другие скорости передачи данных: 6.09.012.018.024.036.048.054.0
5. **Нажмите Apply в нижней части окна.** Пример настройки представлен на следующем окне:

Вопрос. . Действительно ли это истинно, что, если я только позволяю клиентам IEEE 802.11g на беспроводной сети, они не могут вмешаться в параллельную сеть IEEE 802.11b, потому что они используют другие схемы модуляции?

O. Нет, это не истинно. Клиенты 802.11g могут вызывать помехи, если используют ту же частоту, что клиенты IEEE 802.11b. Убедитесь, что сети используют разные каналы. Три неперекрывающихся канала — 1, 6 и 11.

Вопрос. . Какова скорость Порта Ethernet AP?

O. Порт Ethernet AP поддерживает или 10 Мбит/с или 100 Мбит/с по разъёму RJ-45, или в полудуплексном или в полном дуплексе. Необходимо зафиксировать параметры скорости и дуплекса, аналогичные параметрам коммутатора или концентратора.

Вопрос. . Существует ли механизм для аварийного переключения или резервирование для моего AP?

O. Да, можно настроить горячее резервирование для обеспечивания избыточности, если отказывает основной AP. См. Комментарии к выпуску для точек доступа Cisco Aironet для получения дополнительной информации.

Вопрос. . Что такое WEP-ключ?

O. WEP обозначает Безопасность, аналогичная защите проводных сетей. Функцию WEP можно использовать для шифрования и расшифровки сигналов данных, передаваемых между устройствами беспроводной локальной сети (WLAN). WEP — это дополнительная функция IEEE 802.11, которая позволяет предотвратить раскрытие и изменение транзитных пакетов, а также обеспечивает контроль доступа для сети. WEP делает канал WLAN таким же безопасным, как проводной канал. Как указано в стандарте, WEP использует алгоритм RC4 с 40-битным или 10-битным ключом. RC4 является симметричным алгоритмом, так как использует один ключ для шифрования и расшифровки данных. При включении WEP все радиостанции получают ключи. Ключ используется для скремблирования данных перед

передачей в эфир. Если станция получает пакет, который не был скремблирован правильным ключом, она отклоняет пакет и никогда не доставляет его хосту. См. Протокол WEP на Примере конфигурации Точек доступа Aironet и Мостов для получения информации о том, как настроить WEP.

Вопрос. . При использовании Светового расширяемого протокола аутентификации (LEAP) какой номер порта вы задаете для передачи с сервером Cisco Secure Access Control Server (ACS)?

О. По умолчанию ACS слушает запрос аутентификации на порту 1645 и считающий на порту 1646, но можно настроить порт 1812 для аутентификации и 1813 для учета. Убедитесь, что эти порты корректно заданы на странице "Authentication Server Setup" точки доступа.

Вопрос. . В AP на основе ПО Cisco IOS можно ли выполнить статические ключи Протокола WEP и Протокол EAP вместе на том же AP для аутентификации? Это было возможно в точках доступа на базе VxWorks.

О. Нет, вы не можете выполнить статические ключи WEP для шифрования и EAP для аутентификации в том же идентификаторе набора сервисов (SSID). VxWorks позволил эту конфигурацию из-за уязвимости программного обеспечения, но эта способность не является функцией. Для решения этой проблемы создайте два идентификатора SSID и две сети VLAN (по одной на каждый SSID). Затем настройте открытую аутентификацию с использованием WEP для одного SSID и аутентификацию EAP для другого SSID.

Вопрос. . Вы действительно хотите провести обследование места?

О. Да. В связи с чувствительной природой радиочастотной передачи, необходимо получить данные о других типах РЧ-трафика, которые могут присутствовать в среде, даже если вы не знаете об этом. Обследование узла позволяет лучше оценить эту невидимую угрозу для производительности беспроводных устройств. Кроме того, обследование узла позволяет специалисту по установке гарантировать требуемую зону действия РЧ. См. документ Вопросы и ответы по обследованию узла.

Вопрос. . При попытке модифицировать AP, и вам предлагают для имени пользователя и пароля, что вы вводите?

О. Приглашение для имени пользователя и пароля указывает, что включили Менеджеру пользователей. Имя пользователя и пароль можно получить у администратора точки доступа. Если вы являетесь администратором точки доступа и не знаете параметров учетных записей, восстановите пароль. См. документ Процедура восстановления пароля для оборудования Cisco Aironet.

Вопрос. . Можно ли использовать две внешних антенны для покрытия двух радиоячеек (например, антенна 1 для ячейки 1 и антенна 2 для ячейки 2)?

О. Вы не можете использовать две антенны на AP для покрытия двух радиоячеек. Попытка использовать две антенны для покрытия двух сот может привести к возникновению проблем подключения. Две антенны применяются для усиления зоны действия в соте и решения проблем, связанных с искажениями, которые вызваны многолучевым распространением и

замиранием сигналов. Дополнительные сведения об искажениях, связанных с разнесенным приемом и многолучевым распространением сигналов см. в документе Многолучевое распространение и разнесенный прием.

Вопрос. . Каково использование команды mobility network-id на AP?

O. Команда mobility network-id используется для настройки мобильности уровня 3 в беспроводной сети. *Команда mobility network-id ssid используется для привязки идентификатора SSID идентификатору мобильной сети. При использовании мобильной сети уровня 3 клиенты могут переключаться между точками доступа, установленными в различных подсетях, в режиме роуминга.* Клиенты в режиме роуминга сохраняют подключение к сети и не меняют IP-адреса.

Для правильной настройки мобильной сети уровня 3 необходимо назначить модуль WLSM устройством WDS. При использовании точки доступа в качестве WDS, мобильность уровня 3 не поддерживается. *Дополнительные сведения о мобильных сетях уровня 3 см. в разделе Общие сведения о мобильных сетях уровня 3 документа Настройка WDS, быстрого и безопасного роуминга и управления радиомодулями.*

Эту команду необходимо использовать, когда точка доступа входит в инфраструктуру WDS с модулем WLSM (который служит устройством WDS) и с включенной мобильной сетью уровня 3. При использовании эту команду неправильно, неполадки подключения в результате сети WLAN, такие как они:

- Клиенты не получают IP-адреса от DHCP.
- В некоторых случаях, клиенты не могут соединиться с точкой доступа.
- Беспроводной клиент не может установить соединение с точкой доступа.
- Аутентификация по протоколу EAP не выполняется. **Когда команда mobility network-id настроена, точка доступа пытается сформировать туннель GRE для пересылки пакетов EAP.** Если такой туннель не создан, пересылка пакетов невозможна.
- Точка доступа, настроенная как устройство WDS, не работает должным образом и конфигурация WDS не функционирует.

Вопрос. . Сколько идентификаторов наборов сервисов (SSIDs) вы можете иметь на VLAN?

O. У вас может быть только один SSID на VLAN. Использование нескольких идентификаторов SSID в одной сети VLAN в точках доступа Aironet не поддерживается.

Вопрос. . Каково значение BSSID, когда множественный, ESSIDs назначены на AP?

O. Если AP будет работать в облегченном режиме, то каждый ESSID на AP будет обрабатываться через другой BSSID (где каждый BSSID основан на радио-основном MAC и отличается только по откусыванию младшего разряда.)

Если AP выполнит IOS, то весь ESSIDs на AP будет обрабатываться через тот же BSSID (пока MBSSID не будет настроен, в этом случае они будут обрабатываться через другой BSSIDs).

Вопрос. . Действительно ли возможно установить мой радио для моста и радио G для функциональности AP? Если да, то как?

O. Да, возможно установить каждое радио в вашем AP для другой функциональности. Если вы устанавливаете другие идентификаторы наборов сервисов (SSIDs) для G и радио, в вашем сценарии это может быть сделано. Затем установите следующие роли в радиосети, точка доступа (AP) для радиомодуля G и корневой мост (root bridge) для радиомодуля A.

Вопрос. . Когда два клиента связываются к двум другим AP, которые связаны в той же подсети, связь происходит через проводную сеть или происходит с помощью беспроводных технологий?

O. Для этого сценария, если эти два AP установлены в корневой режим, связь между этими двумя AP через проводную сеть. Если одна из точек доступа работает в режиме повторителя, а другая — в режиме root, для связи между ними будет использоваться беспроводной канал.

Вопрос. . Можно ли позволить направить или Технология NAT на AP Cisco?

O. Нет, маршрутизация и Характеристики NAT не поддерживается на AP.

Вопрос. . Когда AP на основе ПО Cisco IOS доступен, существует ли способ планировать время? Я хотел бы предоставить доступ на основе времени суток клиентам, которые подключаются к точке доступа.

O. Можно настроить контрольные списки доступа на основе времени (ACL) с использованием временных диапазонов. Списки ACL на основе времени суток позволяют гарантировать, что пользователи будут получать доступ к беспроводной сети только в заданный период времени, например с 9:00 до 17:00. При использовании ACL на основе времени суток точка доступа и радиомодуль не отключаются. Списки ACL на основе времени суток останавливают прохождение трафика через точку доступа, что не позволяет пользователям получать доступ к сети. *Дополнительные сведения о настройке этой функции см. в разделе Списки ACL на основе времени суток с временными диапазонами документа Настройка списков доступа IP.*

Вопрос. . AP могут иметь множественные пулы DHCP через другие подсети?

O. При настройке AP как сервера DHCP IP-адреса назначены на устройства, которые находятся в той же подсети как сервер DHCP. Устройства взаимодействуют с другими устройствами в подсети, но не имеют доступа к устройствам за ее пределами. Для передачи данных за пределы подсети необходимо настроить маршрутизатор по умолчанию. IP-адрес маршрутизатора по умолчанию должен относиться к подсети, в которой находится точка доступа, настроенная в качества DHCP-сервера.

Вопрос. . Каково измерение дБм? Как определить эквивалентные значения дБм для уровня сигнала (в мВт), который отображается для точки доступа Aironet?

O. ДБ модуля измеряет питание сигнала как функция его соотношения к другому

стандартизированному значению. К аббревиатуре дБ часто добавляются другие аббревиатуры, указывающие на то, какие значения сравниваются. Таким образом, дБм — это значение, которое получается при сравнении дБ со стандартным эталонным значением 1 мВт.

Формула расчета значения дБм для заданного уровня сигнала в мВт выглядит следующим образом:

```
Power (in dB) = 10 * log10 (Signal/Reference)
```

В этом списке объясняются значения формулы. log10 — это десятичный логарифм.

- Сигнал — это мощность сигнала (например, 50 мВт).
- Базой является эталонная мощность (например, 1 мВт).

Пример:

Чтобы рассчитать мощность в дБ для уровня сигнала 50 мВт используйте следующую формулу:

```
Power (in dB) = 10 * log10 (50/1) = 10 *log10 (50) = 10 * 1.7 = 17 dBm
```

Из этой формулы можно вывести следующее общее правило:

- Каждое увеличение уровня на 3 дБ (в этом примере дБм), означает удвоение текущей мощности передачи (в мВт). Каждое уменьшение уровня на 3 дБ означает уменьшение текущей мощности передачи (в мВт) на половину.
- Каждое увеличение уровня на 10 дБ (в этом примере дБм), означает 10-кратное увеличение текущей мощности передачи (в мВт). Каждое уменьшение уровня на 10 дБ означает уменьшение текущей мощности передачи (в мВт) в 10 раз.
- Каждое увеличение уровня на 30 дБ (в этом примере дБм), означает 1000-кратное увеличение текущей мощности передачи (в мВт). Каждое уменьшение уровня на 30 дБ означает уменьшение текущей мощности передачи (в мВт) в 1000 раз.

Эта таблица показывает приблизительное отношение дБм к мВт:

[См. дополнительные сведения в документе Значения мощности РЧ.]

Вопрос. . Как я изменяю настройки даты и времени на AP Cisco 1231?

О. Перейдите к веб-интерфейсу (GUI), выберите **Services> SNTP**, выберите **Time Settings** и затем измените время.

Вопрос. . Если CCKM НЕ будет настроен на клиенте, но будет настроен на AP, то клиент будет в состоянии связаться с AP? Смогут ли клиенты выполнять нормальный роуминг?

О. Поведение зависит от конфигурации AP. Если функция CCKM НЕ настроена или не поддерживается на клиенте, клиент не сможет соединится с точкой доступа, если функция CCKM работает в режиме "mandatory" (обязательно). Если инфраструктура (точка доступа) использует CCKM в режиме "optional" (необязательно), клиент сможет соединиться с точкой доступа и установить связь без использования CCKM.

В зависимости от развертываемых клиентов, рекомендуется устанавливать функцию CCKM

на режим "optional" в инфраструктуре, которая разрешает соединение со всеми устройствами, но поддерживает роуминг ТОЛЬКО для устройств, соединенных с использованием CCKM.

Вопрос. . Каково различие в объеме памяти между AP 1240 и 1230?

O. Это объемы памяти AP 1240 и 1230:

- AP 1240 является AP платформы на 32 МБ.
- 1230 — это точка доступа с платформой 16 МБ.

Вопрос. . У меня есть два 1240-х AP та гибкость роли канала поддержки. Я хотел бы создать между ними мост 802.11a с использованием клиентов, подключенных в диапазонах 802.11b/g. Есть ли какие-то ограничения для этой конфигурации?

O. Гибкость роли ссылки точки доступа оказывает поддержку функциональности мостового режима для точек доступа, которые имеют двухдиапазонную возможность (1200, 1230, и серия 1240AG). В рассматриваемой конфигурации, радиомодуль 802.11a работает в режиме моста, в то время как модуль 802.11g работает в режиме точки доступа.

При конфигурировании точки доступа с функцией гибких ролей, один из радиомодулей необходимо настроить в качестве корневой точки доступа (root AP), вторая точка доступа, которая служит мостом, должна работать в режиме повторителя или WGB по отношению к корневой точке доступа.

Вопрос. . Сколько телефонов беспроводной IP-телефонии рекомендуется на AP?

O. Калибровка сети для IP-телефонии важна, чтобы гарантировать, что достаточная пропускная способность и ресурсы доступны для переноса критически важного голосового трафика. В дополнение к обычным проектным указаниям по определению размера компонентов IP-телефонии, таких как шлюзовые порты PSTN, транскодеры, пропускная способность WAN и др., при определении размера беспроводной сети для IP-телефонии следует учесть следующие вопросы, связанные с 802.11b:

- Количество устройств 802.11b на точку доступа: Cisco рекомендуется использовать не более 15–25 устройств.
- Количество телефонов 802.11b на точку доступа

Перед рассмотрение планов сети, следует понять основные факторы, влияющие на общую производительность сети. При определении размера беспроводной сети для IP-телефонии следуйте нижеперечисленным указаниям по производительности сети:

- Не более 7 параллельных вызовов на точку доступа G.711
- Не более 8 параллельных вызовов на точку доступа G.729

Примечание: В этих проектных рекомендациях предполагается, что функция VAD беспроводных IP-телефонов Cisco 7920 была отключена.

Использование VAD на телефонах Cisco 7920 экономит пропускную способность, но Cisco рекомендует отключать VAD на всех серверах Cisco CallManager для улучшения общего

качества голоса. Помимо пропускной способности, необходимой для VoIP-вызовов 802.11b, необходимо учесть уровень конфликтов в отдельно взятом канале РЧ. Общее правило гласит, не следует развертывать больше 20–25 терминалов 802.11b на точку доступа. С увеличением количества терминалов на точку доступа уменьшается общая пропускная способность и, вероятно, увеличиваются задержки передачи. Максимальное количество телефонов на точку доступа зависит от схем вызовов отдельных пользователей (на основе соотношений Эрланга). Cisco рекомендует ограничение на 7 параллельных вызовов для точки доступа G.711 и 8 параллельных вызовов для точки доступа G.729. Если это ограничение будет превышено и плотность фонового потока данных будет высока, качество голоса на всех вызовах станет неприемлемым. Скорости преобразования данных в пакеты для этих рекомендаций базируются на выборках 20 мс с отключенной функцией VAD. Эта выборка формирует 50 пакетов в секунду в обоих направлениях. Больший размер выборки (например 40 мс) позволит увеличить число параллельных вызовов, но при этом увеличит сквозную задержку для вызовов VoIP.

Количество телефонов 802.11b , которое можно развернуть в одной подсети или VLAN уровня 2 зависит от следующих факторов:

- Используйте не более 7 вызовов G.711 или 8 вызовов G.729 на точку доступа.
- Для определения активных и неактивных вызовов используется параметр "отношение вызова". Это соотношение как правило определяется с помощью калькуляторов Эрланга. Основываясь на этих факторах, а также на нормальных соотношениях Эрланга бизнес-класса (между 3:1 и 5:1), Cisco рекомендует развертывать не более 450–600 телефонов Cisco 7920 на подсеть или сеть VLAN уровня 2.

Более подробные сведения см. в разделе Определение размера сети документа Инфраструктура беспроводной сети, а также в документе Готова ли сеть WLAN для передачи голоса.

Вопрос. . Как я могу мешать AP 1200 обработать запросы аутентификации после количества набора попыток?

О. Можно использовать опцию максимальных чисел повторных попыток на AAA-сервере для ограничения числа раз, клиенты могут попытаться обратиться к сети. Значение этого параметра можно настроить вручную на сервере AAA или использовать количество попыток по умолчанию, которое зависит от используемого сервера AAA.

Вопрос. . Где я могу найти информацию о различиях в различных платформах AP и LAP?

О. См. Часто задаваемые вопросы беспроводного оборудования Cisco. Этот документ содержит полезные сведения, которые сравнивают другой AP и модели LAP.

Вопрос. . Протокол PPPoE поддерживается в точках доступа Cisco Aironet?

О. Нет, PPPoE не поддерживается в точках доступа Cisco Aironet.

Вопрос. . Протокол магистральных каналов VLAN (VTP) поддерживается в точках доступа Cisco Aironet?

О. Нет, VTP не поддерживается в точках доступа Cisco Aironet.

Вопрос. . Точка доступа Cisco Aironet поддерживает 802.11f стандартный Протокол межточки доступа (IAPP)?

O. Нет, точка доступа Cisco Aironet не поддерживает 802.11f основанный IAPP. Точки доступа Cisco предлагают свое собственное устойчивое, с расширенными возможностями, и доказанный протокол межточки доступа.

Вопрос. . Каковы использование `bridge-group 1` И `bridge-group 1 source-learning` В AP?

O. Используйте команду настройки интерфейса **bridge-group block-unknown-source** для блокирования трафика от неизвестных MAC-адресов на определенном интерфейсе. Не используйте форму команды для отключения неизвестного источника, блокирующегося на определенном интерфейсе.

Для STP для функционирования должным образом **блочный неизвестный источник** должен быть отключен для интерфейсов, которые участвуют в STP.

```
bridge-group group block-unknown-source
```

Когда вы включаете STP на интерфейсе, **блочный неизвестный источник** отключен по умолчанию.

Команда bridge-group 1 source-learning заставляет AP изучить адрес источника клиента. Не используйте форму команды для отключения AP от обучения адреса источника клиента.

Вопрос. . Существует ли способ расположить по приоритетам трафик, который течет через AP так, чтобы трафик от определенного SSID, настроенного на AP, использовал более высокую пропускную способность, чем другой SSIDs на том же AP?

O. Это может быть достигнуто с реализацией Качества обслуживания (QoS) на AP.

- Создайте политики QoS и примените политику к VLAN, настроенным на вашей точке доступа. Эти документы объясняют QoS и как настроить политики QoS на AP.Беспроводное качество обслуживанияQoS Настройки на точках доступа Aironet
- Затем сопоставьте SSIDs, настроенный на AP к упомянутым отдельным VLAN. Таким образом при расположении по приоритетам трафика на основе VLAN можно, в свою очередь, расположить по приоритетам трафик на основе SSID.

Вопрос. . Существует ли способ ограничить максимальное число устройств клиента, которые могут соединиться с одиночной Автономной точкой доступа?

O. Поведение по умолчанию устройства клиента Cisco - то, что оно соединяется с AP, который имеет лучший уровень сигнала в наличии. Но можно ограничить клиентов, которые могут соединиться с каким-то конкретным AP посредством проверки подлинности MAC. Необходимо предоставить MAC-адрес клиента к AP так, чтобы AP мог позволить только тем клиентам и ограничить всех других клиентов, которые не являются частью списка разрешенного адреса MAC от соединения до того определенного AP.

Вопрос. . От того, где можно загрузить последние версии программного обеспечения?

О. Оборудование CISCO Aironet работает лучше всего при загрузке всех компонентов актуальнейшей версией ПО. Последние версии драйверов и программного обеспечение можно загрузить на веб-узле Cisco Wireless Software Center (только для зарегистрированных заказчиков).

Вопрос. . Действительно ли необходимо отключить все портативные ПК и другие беспроводные устройства во время обновления точки доступа?

О. Нет, нет никакой потребности отключить устройства. Обновление точки доступа — безопасный процесс и все устройства могут оставаться включенными. Убедитесь, что существует подключение к серверу TFTP.

Вопрос. . Где я могу найти инструкции по тому, как обновить Cisco IOS® на AP Cisco Aironet?

О. См. Работу с Образами программного обеспечения для инструкций по тому, как обновить Cisco IOS на AP.

Примечание: Используйте опцию **повторной загрузки силы** с **командой archive download-sw**.

Примечание: Когда вы обновляете AP или соединяете системное программное обеспечение путем ввода **команды archive download-sw** в CLI, необходимо использовать опцию **повторной загрузки силы**. Если AP или мост не повторно загружают флэш-память после того, как обновление, страницы в интерфейсе вебе - обозревателе не могли бы отразить обновление. Данный пример показывает, как обновить системное программное обеспечение при помощи **команды archive download-sw**:

```
AP#archive download-sw /force-reload / overwrite tftp://10.0.0.1/image-name
```

Вопрос. . У меня есть AP 1100 года. Необходимо обновить радиомодули точки доступа с IEEE 802.11b до IEEE 802.11g. Если я обновлю радиомодуль точки доступа, смогу ли я использовать существующие платы для компьютеров? Или платы для компьютера также нуждаются в обновлении? В настоящий момент используются платы 802.11b.

О. Если вы только используете 802.11b клиенты, обновление 802.11b радио к 802.11g не приводит ни к какому повышению производительности. Преимущество обновления радиомодуля до 802.11g заключается в поддержке подключения к точке доступа как для клиентов 802.11b, так и для клиентов 802.11g. После обновления клиенты 802.11b будут подключаться на скорости 11 Мбит/с, а клиенты 802.11g — на скорости 54 Мбит/с.

Вопрос. . Как вы задерживаете AP к его заводским настройкам?

О. См. документ Процедура восстановления пароля для оборудования Cisco Aironet.

Вопросы по поиску и устранению неисправностей

Вопрос. . Я сделал некоторые изменения конфигурации к AP. Когда я пытаюсь сохранить изменения, точка доступа выдает следующее сообщение: **"Error writing new config file "flash:/config.txt.new" nv_done: unable to open "flash:/config.txt.new" nv_done: unable to open "flash:/private-multiple-fs.new"[OK]".** Что означает это сообщение?

О. Это сообщение об ошибках указывает, что нет никакого пространства во Флэше для хранения новой конфигурации. Попробуйте удалить старые файлы сбоев. Или, если в памяти присутствует несколько версий ПО Cisco IOS, удалите неиспользуемые версии. Это поможет освободить место во Flash-памяти. **Введите команду dir flash, чтобы выявить старые файлы исключений crashinfo, которые можно удалить, или неиспользуемые старые образы. Введите команду write memory, чтобы освободить место. Это позволит записать конфигурацию в память.**

Вопрос. . Я использую Aironet Client Utility (ACU) 6.3 и точки доступа Cisco 1200 (AP), которые выполняют программное обеспечение Cisco IOS версии 12.3 (8) JA. Когда беспроводной клиент присоединяется к точке доступа, имя точки доступа не отображается в приложении ACU. В чем причина?

О. Название AP является именем хоста для AP. Если расширения Aironet включены на точке доступа, ее имя будет отображаться в приложении ACU.

Если вы не хотите, чтобы имя точки доступа отображалось, отключите расширения Cisco Aironet для стандарта IEEE 802.11b (параметр no dot11 extensions aironet в интерфейсе радиомодуля). По умолчанию расширения Cisco Aironet активны на точках доступа.

Если расширения Cisco Aironet были отключены ранее, их можно включить с помощью следующей команды:

```
AP(config-if)#dot11 extension aironet
```

Точки доступа добавляют в сигналы-маяки проприетарный информационный элемент Cisco, который содержит имя точки доступа. Если вы отключите расширения Aironet на точке доступа, она не будет добавлять свое имя в сигналы-маяки. Дополнительные сведения о расширениях Aironet см. в документе Отключение и включение расширений Aironet.

Вопрос. . Моя точка доступа (AP) принимает и соединяется только с одним клиентом за один раз. В чем причина?

О. Одна возможная причина могла быть то, что параметр **max-associations** установлен на 1 под идентификатором набора сервисов (SSID) конфигурация. **Введите команду max-associations в режиме конфигурации SSID, чтобы настроить максимальное количество соединений, поддерживаемых радиоинтерфейсом (для указанного SSID). Используйте команду в формате no, чтобы сбросить параметр в значение по умолчанию.** Максимальное значение этого параметра по умолчанию — 255.

Вопрос. . Как можно восстановить забытые пароли?

О. См. документ Процедура восстановления пароля для оборудования Cisco Aironet.

Вопрос. . Серийные номера не обнаруживаются ни на одном BR350 или

AP350, которые мы имеем командами. Это точки доступа VxWorks, которые не были преобразованы в IOS. Как я получаю эту информацию из устройств?

O. AP серии 350 и Бриджес, которые выполняют VxWorks, не отображают серийный номер в программном обеспечении. Единственный способ определить серийный номер этих устройств — прочитать его на наклейке на самих устройствах.

Вопрос. . Что такое возможные источники интерференции для ссылки радиочастот (RF) AP?

O. Интерференция может прибыть из многих источников, таких как:

- беспроводные телефоны 2,4 ГГц
- Микроволновые печи с плохим экранированием
- Беспроводное оборудование других производителей

Электродвигатели и подвижные металлические части механизмов также могут вызывать помехи. Дополнительные сведения см. в следующих документах:

- Поиск и устранение проблем, влияющих на радиочастотную связь
- Проблемы пропадающего подключения в беспроводных мостах

Вопрос. . Я вижу сообщение об ошибках: %C4K_EBM-4-HOSTFLAPPING:Host [MAC - адрес] в vlan [цифра] колеблется между портом [цифра] и портом [цифра], связанная с точками доступа. Как мы решаем это?

O. Когда коммутатор изучает тот же MAC-адрес через множественные порты, это сообщение об ошибках происходит. Это может произойти из-за одной из этих причин

1. Когда клиент перемещается от одного AP до другого AP, новый AP сообщает клиенту MAC-адреса к коммутатору. Если оба, AP связаны с тем же коммутатором, MAC-адресом клиента, привязаны к обоим порты коммутатора, связанные с AP. Это создает дублированную запись для клиента и генерирует это сообщение об ошибках до времени, когда коммутатор синхронизирует свою таблицу CAM. Это сообщение об ошибках довольно обычно в Беспроводной среде, но, если слишком много роуминга происходит, это может перегрузить ЦП коммутатора. Проверьте драйвер клиента и микропрограммное обеспечение. Кроме того, гарантируйте, что покрытие хорошо так, чтобы клиент часто не перемещался.
2. Когда существует петля, коммутатор может изучить тот же MAC-адрес через множественные порты, связанные с другими коммутаторами. Гарантируйте, что TP включен на коммутаторе.

Вопрос. . Почему случается так, что клиентская карта не связывается к самому близкому AP?

O. Если существуют множественные AP в вашей беспроводной топологии, ваш клиент поддерживает ассоциацию с AP, с которым первоначально связался клиент, пока клиент не теряет сигналы-маяки поддержки активности от того AP. Если связь потеряна и попытки восстановить связь с исходной точкой доступа заканчиваются неудачей, клиент начинает

искать другую точку доступа. Клиент пытается соединиться с новой точкой доступа, если у него достаточно прав и он авторизован на данной точке доступа.

Вопрос. . У меня есть AP Cisco и сервер Cisco Secure Access Control Server (ACS) 3.2. В сети применяется протокол EAP. Аутентификация пользователей выполняется сервером RADIUS. При вводе команд отладки на точке доступа я получаю следующие выходные данные: "Jun 2 15:58:13.553: %RADIUS-4-RADIUS_DEAD: RADIUS server 10.10.1.172:1645,1646 is not responding. "Jun 2 15:58:13.553: %RADIUS-4-RADIUS_ALIVE: RADIUS server 10.10.1.172:1645,1646 has returned. Jun 2 15:58:23.664: %DOT11-7-AUTH_FAILED: Station 0040.96a0.3758 Authentication failed.". ?

O. Одна из причин, почему эти сообщения об ошибках появляются, - то, что общий секретный ключ не является тем же в AP и ACS. Эта ошибка часто встречается во время настройки EAP. Если ключи точки доступа и сервера ACS 3.2 не совпадают, протокол EAP работать не будет. Сервер RADIUS не принимает пакеты, которые пересылает точка доступа. Убедитесь, что общий секрет точки доступа совпадает с общим секретом сервера ACS. Для получения информации о том, как отладить, обратитесь к Debug authentication.

Вопрос. . Когда я просмотрел вход в систему AP, я нашел эту ошибку: "Mar 9 11:05:26.225 Information Group rad_acct: Radius server 10.10.1.172:1645,1646 is responding again (previously dead). Mar 9 11:03:09.361 Error Group rad_acct: No active radius servers found.". ?

O. Когда **radius-server deadtime** установки настроен на AP, это обычно для наблюдения этого журнала. Это информационная запись журнала, которая не представляет серьезной проблемы. **Команда radius-server deadtime позволяет установить интервал, в течение которого точка доступа не будет предпринимать попытки связаться с неотвечающими серверами. В результате точке доступа не придется ждать окончания времени ожидания запроса, чтобы попытаться подключиться к следующему настроенному серверу.** Дополнительные запросы не будут отправляться серверу, который отмечен как "dead" (простаивающий), в течение указанного периода времени в минутах. Максимальное значение этого периода составляет 1440 мин (24 ч).

Вопрос. . У меня есть AP 1230 с программным обеспечением Cisco IOS версии 12.3 (4) JA. ACL "% Warning: Saving this config to nvram may corrupt any network management or security files stored at the end of nvram. ? :"

O. Это - предупреждающее сообщение и не ошибка. Если вы выберите [no], данные не будут сохранены на точках доступа. Конфигурации сохраняются не в энергонезависимой памяти (NVRAM), а во Flash-памяти.

Несмотря на то что это только предупреждение, в памяти точки доступа существует проблема. В ней сохранено несколько RCORE-файлов, которые занимают много места. Пример представлен в выходных данных:

```
3 -rwx 262144 Mar 3 2002 22:40:04 +00:00 r13_5705_9760_1EA7A81E.rcore

4 -rwx 262144 Mar 1 2002 17:21:44 +00:00 r13_5705_9760_709D16F4.rcore

5 -rwx 262144 Mar 7 2002 20:19:12 +00:00 r13_5705_9760_9D2DE9CD.rcore

6 -rwx 262144 Mar 26 2002 23:42:22 +00:00 r13_5705_9760_AAE78172.rcore

151-rwx 262144 Mar 1 2002 17:22:00 +00:00 r13_5705_9760_7187935C.rcore
```

Чтобы очистить память, удалите все RCORE-файлы из Flash-памяти.

Ниже приведен пример команды, которую необходимо ввести в режиме "enable":

```
ap#delete flash:r13_5705_9760_1EA7A81E.rcore
```

Примечание: Выполните этот **удалите флэш-память:** для каждого RCORE-файла во Flash-памяти.

Вопрос. . У меня есть модуль служб беспроводной сети (WLSM) с Cisco IOS Software Release 12.4 (4) установленный T1. Подключения к клиентам обрываются. Просматривая журналы я нахожу сообщения следующего содержания "Previous authentication no longer valid" и "Disassociated because sending station is leaving (or has left) BSS". В чем проблема?

О. Оба из этих сообщений указывают к проблеме RF. Чтобы устранить проблему, назначьте точке доступа другие каналы.

Вопрос. . AP Cisco Aironet в моей сети WLAN не передают идентификаторы наборов сервисов (SSIDs). В чем причина? Нужно ли включить определенную функцию в точке доступа?

О. Пока вы не включаете Гостевой режим при Диспетчере SSID, AP не передает SSID в своих сигналах-маяках. Это можно проверить с помощью клиента, просканировав сеть, чтобы убедиться, что идентификаторы SSID не отображаются.

Чтобы включить гостевой режим SSID, введите следующую команду в режиме глобальной конфигурации точки доступа:

```
Ap<config>#dot11 ssid ssid-string Ap<config-ssid>#guest-mode
```

Вопрос. . У меня есть свой AIR-AP1231G-A-K9 AP. Почему я не вижу параметр, включающий радиомодуль A на этой точке доступа, и отображаются только параметры радиомодулей G? Можно ли соединить клиенты 802.11b с этой точкой доступа?

О. AIR-AP1231G-A-K9 AP имеет радио G. Номер детали AP1231G указывает на то, что она поставляется только с радиомодулем G. Радиомодули G имеют обратную совместимость с радиомодулями B, так как они используют одинаковую частоту. Но радиомодуль A отсутствует в устройстве, и поэтому его нельзя включить. При необходимости радиомодуль A можно добавить в точку доступа. Радиомодуль A работает на частоте 5 ГГц, в то время как радиомодули G и B работают на частоте 2,4 ГГц.

Вопрос. . У меня есть IP-телефон беспроводной связи Cisco 7920, который связан с AP Cisco. IP-телефон 7920 соединяется с точкой доступа, но IP-адрес не назначается. Я использую протокол EAP. Я вижу сообщение " **[SEP001121ceb9a4] 001121ceb9a4, ", который придерживается " [SEP001121ceb9a4] 001121ceb9a4 c" И " EAP, [SEP001121ceb9a4] 001121ceb9a4". "Info Deauthenticating [SEP001121ceb9a4]001121ceb9a4, reason 'Previous Authentication No Longer Valid' ". В чем проблема?**

О. Причина, что вы получаете эти сообщения, состоит в том, что общий секретный ключ в AP отличается, чем общий секретный ключ от сервера RADIUS. Убедитесь, что общие секреты для аутентификации EAP одинаковы. Повторно введите общий секрет на точке доступа и сервере RADIUS.

Вопрос. . У меня есть проблема с моим AP. Она отправляет слишком много сообщений RTS в режиме очереди, что приводит к непредвиденному отсоединению и присоединению клиентов. Клиенты были соединены с этой точкой доступа при уровнях сигнала -91 и -95 дБм. В чем причина непредвиденного отсоединения? Является ли это ожидаемым поведением устройства?

О. Да, это - нормальное поведение. Ваш клиент находится на краю соты 1 Мбит/с. На уровнях -91 to -95 дБм такое хаотичное поведение является ожидаемым.

Чтобы решить эту проблему, установите дополнительные точки доступа. Или, если необходима сосредоточенная зона действия, а не всенаправленная, используйте направленные антенны.

Рассылка сообщений RTS вызвана механизмами повтора. В ответ на сообщение RTS клиент должен отправлять сообщение CTS, но если клиент видит эти сообщения в анализаторе трафика как 8 кадров RTS без соответствующего кадра CTS, он не воспринимает точку доступа или находится слишком далеко, чтобы точка доступа могла воспринимать его. Устройства должны воспринимать друг друга; если точка доступа воспринимает клиент, но клиент не воспринимает точку доступа, этого недостаточно для нормальной работы. Таким образом, если антенна клиента несовершенна (а это возможно) или его передатчик не поддерживает уровень 100 мВт (вполне вероятно) или чувствительность клиента значительно превышает -90 to -95 дБм (почти наверняка, если клиент произведен не Cisco), поведение сети будет именно таким, как вы описали.

Вопрос. . Мы используем AP беспроводных сетей LWAPP Cisco. Я наблюдаю множество операций повторной передачи TCP и дублированных ACK на клиентах, но ничего подобного не происходит в проводной среде. Это нормально для беспроводной сети?

О. Поврежденные пакеты и ретранслируемые пакеты являются двумя из фундаментальных метрик WLAN 802.11. Анализ поврежденных и повторно отправленных пакетов в 802.11отличается от аналогичного анализа для проводных локальных сетей по трем причинам:

- Во-первых, сети 802.11 WLAN как правило производят гораздо больше поврежденных пакетов, чем проводные локальные сети, поэтому важность поврежденных кадров в сети 802.11 WLAN повышается.
- Во вторых, сети 802.11 определяют уровень надежного канала данных. Это значит, что каждый поврежденный пакет должен быть передан повторно. Проводные локальные сети как правило не определяют уровень надежного канала данных и повторная передача происходит только при использовании надежного протокола.
- И наконец, надежность высокого уровня, как правило, является сквозной. Это означит, что поврежденный пакет в любом элементе тракта между источником и назначением

становится причиной повторной передачи. Повторная передача 802.11 происходит на уровне 2 и внедряется между проводными интерфейсами, таким образом повторная передача 802.11 может быть вызвана только повреждением в локальном "сегменте". Это делает обнаружение повреждений в сетях 802.11 WLAN значительно проще, чем аналогичный процесс в традиционных проводных локальных сетях. Рассмотрим некоторые последствия этих различий.

Одна из главных задач беспроводных сред — убедиться, что анализатор получает те же данные, что клиенты. Различия в радиомодулях, антеннах и расположении клиента и анализатора могут привести к тому, что они будут принимать разные данные. Например, если анализатор находится далеко от точки доступа, а клиент — близко, анализатор примет поврежденный кадр, в то время как кадр, принятый станцией, будет нормальным. Зная, что каждый поврежденный кадр вызывает повторную передачу, мы можем использовать отношение числа операций повторной передачи и числа поврежденных кадров, чтобы оценить степень соответствия данных, которые принимает анализатор, данным, принимаемым станцией (станциями) в сети.

Вопрос. . Мы видим это широковещание сообщения системного журнала в нашей сети. Почему это происходит, и как мы останавливаем его?

AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: Decode Msg: could not match WLAN <id>

O. Эти сообщения являются предупреждающими сообщениями и замечены, когда Замена WLAN включена, и определенный ИДЕНТИФИКАТОР WLAN не выбран или объявлен на слоте/радио.

Вопрос. . Когда я обновляю свой AP с помощью сервера TFTP, у меня есть проблемы. Каждый раз, когда я пытаюсь обновить, это добавляет расширение .tar к файлу c1200-k9w7-tar.default образа обновления, которые заставляют AP не распознавать файл. Я не мог найти способ избавиться от дополнительного расширения .tar. (Я загрузил и попробовал и solarwind и tftpd32.), Что я должен сделать для устранения этой проблемы?

O. Проблема могла состоять в том, что Операционная система скрывает известный тип файла. Перейдите **к Моему компьютеру**. Нажмите **Tools> Folder Options> View**, прокрутите вниз, пока вы не находите, что параметр **Скрывает расширения для известных типов файла** и снимает флажок. Это должно устранить проблему.

Вопрос. . Мои точки доступа часто встречаются с аварийным сообщением "высокой загрузки ЦП". В таких случаях аппаратная перезагрузка возвращает точку доступа в рабочие условия. Как я могу преодолеть эту проблему?

O. Существует несколько причин для точек доступа для достижения "высокой загрузки ЦП".

- Если точка доступа Cisco (AP) связана с сетью через коммутатор, иногда "высокая загрузка ЦП" наблюдается относительно AP. Это вызвано тем, что, по умолчанию, все VLAN позволены на AP от коммутатора, до которого связан AP. Это может создать проблему, особенно, когда применено к огромная сеть. Если все VLAN позволены на AP, он может привести к **высокой загрузке ЦП**, и на подключение можно влиять. Клиенты, привязанные к точке доступа, сталкиваются с проблемами пропускной способности, и иногда высокая загрузка ЦП может также перевести Беспроводную сеть

в нерабочее состояние.Во избежание этой проблемы сократите VLAN в коммутаторе так, чтобы только трафик виртуальной локальной сети (VLAN), которым интересуется AP, передали через AP.
- Если точки доступа настроены с интерфейсами обратной связи, иногда "высокая загрузка ЦП" наблюдается относительно AP. Несмотря на то, что интерфейсы обратной связи могут быть настроены на AP Cisco, они не поддерживаются на AP, таким образом, они не должны быть настроены. Рекомендуется удалить интерфейсы обратной связи, если они настроены на AP.**Примечание:** AP и мосты не поддерживают команду interface loopback.

Как первый шаг в решении этой проблемы, выполните **команду show process cpu** в AP. Это дает вам общее представление о том, какие процессы используют ЦП.

Кроме того, если AP выполняет версию ранее, чем 12.3 (2) JA2, обновите его к версии 12.3 (2) JA2, потому что существует известная неполадка в более ранних версиях, где запросы на обслуживание уничтожили ЦП.

Вопрос. . Маршрутизатор Wi-Fi на 871 Вт отбрасывает установленные сеансы Wi-fi так, чтобы сеанс VPN пользователя был восстановлен все время. Почему?

О. Существует несколько возможных причин, которые могут вызвать эту проблему. Подключите обоих антенны с маршрутизатором на 871 Вт. Переключите канал к 1, 6 или 11 и проверьте, какой канал получает лучшую производительность. Кроме того, у вас могли бы быть другие AP в окружении, которое может вызывать интерференцию. Это - просто одна возможная причина.

Дополнительные сведения

- Cisco Downloads для беспроводных продуктов (зарегистрированный только клиенты)
- Вопросы и ответы Cisco Aironet серии 1240 AG
- Вопросы и ответы Cisco Aironet серии 1230 AG
- Руководство по конфигурации программного обеспечения точки доступа Cisco Aironet для VxWorks
- Руководство по настройке ПО Cisco IOS для точек доступа Cisco Aironet версии 12.2(13)JA
- Технические примечания по поиску и устранению проблем Cisco Aironet серии 350
- Поддержка беспроводного продукта
- Cisco Systems – техническая поддержка и документация