



Вопросы и ответы по точкам доступа Cisco Aironet

Драйверы, микропрограммы и служебное программное обеспечение доступны на web-сайте Cisco Wireless Software Center (только для зарегистрированных заказчиков).

Вопросы

[Введение](#)
[Вопросы и ответы](#)
[Дополнительные сведения](#)

Введение

Данный документ содержит ответы на часто задаваемые вопросы по точкам доступа Cisco Aironet.

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Вопросы и ответы

Вопрос. Где можно загрузить последние версии программного обеспечения?

Ответ. Оборудование Cisco Aironet работает с наибольшей эффективностью, когда на всех компонентах установлены последние версии ПО. Последние версии драйверов и программного обеспечения можно загрузить на web-сайте Cisco Wireless Software Center (только для зарегистрированных заказчиков).

Вопрос. Нужно ли отключать все переносные компьютеры и другие беспроводные устройства во время обновления точки доступа?

Ответ. Нет, отключать устройства не нужно. Обновление точки доступа — безопасный процесс и все устройства могут оставаться включенными. Убедитесь, что существует подключение к серверу TFTP.

Вопрос. Какое имя и пользователя и пароль по умолчанию используют точки доступа на базе ПО Cisco IOS®?

Ответ. Точки доступа на базе ПО Cisco IOS поставляются с конфигурацией по умолчанию, в которой в качестве имени пользователя пароля используется слово **Cisco** (регистр учитывается). 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 нужно использовать для подключения консоли?

Ответ. Используйте прямой кабель с 9-контактными разъемами "мама" и "папа" для подключения порта COM1 или COM2 компьютера к порту RS-232 точки доступа. На компьютере необходимо запустить программу эмуляции терминала, например:

- Microsoft Windows HyperTerminal
- Symantec ProComm
- Minicom

Используйте следующие параметры портов:

Speed:	9600 bits per second (bps)
Data bits:	8
Stop bits:	1
Parity:	None
Flow Control:	Xon/Xoff

Примечание: Если параметр управления потоком "Xon/Xoff" не работает, попробуйте использовать параметр "None".

Вопрос. Я использую точку доступа Aironet 1231. Производит ли Cisco кабель расширения длиной 50 футов, который позволяет устанавливать точку доступа и антенну в разных помещениях?

Ответ. Да, номер модели 50-футового кабеля — AIR-CAB050LL-R. С помощью этого кабеля можно подключить точку доступа к антенне.

Вопрос. Я внес несколько изменений в конфигурацию точки доступа. 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?

Ответ. Это сообщение указывает на то, что во Flash-памяти недостаточно места для сохранения 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. Как установить IP-адрес для точки доступа?

Ответ. По умолчанию точка доступа запрашивает IP-адрес через DHCP.

Однако, IP-адрес точки доступа можно установить и вручную. 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: Выражение *a.b.c.d* обозначает IP-адрес, который необходимо присвоить точке доступа, *00-12-34-56-78-90* — это 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: Эта процедура не работает в точках доступа, которым IP-адрес уже присвоен с помощью другого метода.

Для точек доступа под управлением VxWorks, IP-адрес можно задать вручную на странице "express setup". Дополнительные сведения см. в документе Конфигурация и базовые параметры радиомодулей.

В точках доступа под управлением ПО Cisco IOS можно вручную задать IP-адрес через web-интерфейс или интерфейс командной строки (CLI). См. раздел *Назначение IP-адреса с помощью CLI* документа Первая настройка точки доступа.

Вопрос. Как клиент выбирает точку доступа для соединения?

Ответ. Точка доступа выбирается в радиомодуле клиента. В зависимости от производителя, драйвера, типа платы и других параметров, радиомодуль может использовать различные метрики для выбора точки доступа. Самый простой механизм присоединения точек доступа, используемый в большинстве клиентов, основывается на уровне сигнала, который клиент получает от точки доступа. Стандарт 802.11 требует, чтобы беспроводной клиент сообщал об уровне сигнала с помощью простой метрики 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. Как расширить зону действия точки доступа?

Ответ. Существует несколько способов расширить зону действия точки доступа. 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.
- изменение параметра мощности передатчика существующей точки доступа для увеличения зоны действия.
- установка точек доступа в оптимальном положении.

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

Вопрос. Каковы последствия работы точки доступа в режиме повторителя?

Ответ. В режиме повторителя порт Ethernet отключается. Полезная пропускная способность уменьшается на половину при каждом переходе от родительской точки доступа.

Вопрос. Можно ли соединить два компьютера без точки доступа с помощью плат беспроводного интерфейса?

Ответ. 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 в режиме ad hoc становятся дочерними станциями.

Вопрос. Требуется ли специальное оборудование для поддержки шифрования?

Ответ. Уровень шифрования в устройстве зависит от его модели.

- Модели 341 и 351 поддерживают 40-битное 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. Можно ли получить информацию обо всех точках доступа и связанных с ними клиентах, принадлежащих к одной сети или инфраструктуре, из одной точки доступа?

Ответ. Это можно сделать из точки доступа VxWorks. Одна точка доступа VxWorks может отображать информацию обо всех клиентах и точках доступа в сети. Для этого выберите **Association > Entire Network > Apply**. В точках доступа на базе IOS все данные обо всех связанных клиентах отображаются только с помощью управляющего устройства, например WLSE с использованием одной точкой доступа в качестве WDS или контроллера, если в точке доступа установлен образ LWAPP.

Вопрос. В сети используется технология ССКМ, но каждый раз, когда клиентское устройство переходит в режим роуминга, выполняется полная аутентификация. Т. е. функции быстрого и безопасного роуминга не работают. Почему?

Ответ. Возможно, проблема вызвана ошибкой в CSCsg10128. Эта ошибка исправлена в версии 3.1.03.

Вопрос. Поддерживают ли точки доступа Cisco функцию UDLD, которая позволяет закрыть Ethernet-подключение к коммутаторам при отказе кабеля уровня 1 или 2?

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

Вопрос. Как обеспечивается питание точек доступа Aironet?

Ответ. Варианты питания точки доступа зависят от конкретной модели. Дополнительные сведения см. в документе Варианты питания для точек доступа Cisco Aironet и контроллеров WLC.

Вопрос. Я использую приложение Aironet Client Utility (ACU) 6.3 и точки доступа Cisco 1200 под управлением ПО Cisco IOS версии 12.3(8)JO. Когда беспроводной клиент присоединяется к точке доступа, имя точки доступа не отображается в приложении ACU. Почему?

Ответ. В поле **AP Name** отображается имя хоста для точки доступа. 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 принимает и подключается только к одному клиенту за раз. В чем причина?

Ответ. Одна из возможных причин — установка значения **1** параметра **max-associations** в конфигурации SSID. 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. Я использую точки доступа AP1010, AP1030 и AIR-LAP-1232AG. Могут ли они использовать модуль WS-PWR-PANEL для питания через Ethernet (PoE)?

Ответ. WS-PWR-PANEL поддерживает только точки доступа с одним радиомодулем. Дополнительные сведения см. в разделе Cisco PoE и Cisco IPM документа Примечание по применению Cisco Aironet PoE.

Вопрос. Как сохранить конфигурацию точки доступа?

Ответ. Изменения конфигурации сохраняются немедленно. Конфигурацию можно сбросить в текстовый формат из меню **Setup**. После этого выберите **Cisco Services > Manage System Configuration** и загрузите конфигурацию системы.

Вопрос. Как определить частоту или каналы, которые используются в точке доступа или мосте?

Ответ. Используйте команду **show controllers dot11Radio0**, чтобы отобразить частоту и канал, на которых работает точка доступа. 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
```

В: Как настроить точку доступа на работу с другими устройствами IEEE 802.11b

Ответ. Чтобы точка доступа могла взаимодействовать с другим устройством 802.11b, необходимо отключить 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 соединяться с точкой доступа?

- 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. На какой частоте работает точка доступа?

Ответ. В США точки доступа, совместимые со стандартом IEEE 802.11b, могут передавать и принимать данные на одном из 11 каналов на частоте 2,4 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 обеспечивается безопасность данных в радиоканале точки доступа?

Ответ. Существует несколько методов защиты данных в беспроводных каналах точки доступа. Дополнительные сведения о различных методах обеспечения безопасности см. в документе Вопросы и ответы по безопасности Cisco Aironet

Вопрос. Как восстановить забытые пароли?

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

Вопрос. Сколько клиентов может соединиться с точкой доступа?

Ответ. Физически точка доступа может обрабатывать до 2048 MAC-адресов. Однако если точка доступа является общим средством связи и используется в качестве беспроводного концентратора, производительность каждого пользователя снижается по мере увеличения количества пользователей отдельной точки доступа. В идеале к точке доступа следует присоединять не более 24 клиентов, так как пропускная способность точки доступа сокращается с каждым присоединенным клиентом.

Вопрос. Существует ли ограничение на количество фильтров MAC-адресов, которые можно настроить на точке доступа?

Ответ. С помощью интерфейса командной строки (CLI) можно настроить до 2 048 MAC-адресов для фильтрации. Однако, при использовании web-интерфейса для фильтрации можно настроить не более 43-адресов.

Вопрос. Серийные номера точек доступа BR350 и AP350 не выводятся при вводе соответствующих команд. Это точки доступа VxWorks, которые не были преобразованы в IOS. Как извлечь эту информацию из устройств?

Ответ. Точки доступа и мосты серии 350 под управлением VxWorks не отображают серийный номер в программном обеспечении. Единственный способ определить серийный номер этих устройств — прочитать его на наклейке на самих устройствах.

Вопрос. Какова стандартная дальность действия для точки доступа?

Ответ. Ответ на этот вопрос зависит от многих факторов, в том числе:

- необходимая скорость передачи данных (пропускная способность)
- тип антенны
- длина кабеля антенны
- устройство-приемник

При оптимальной установке дальность действия может достигать 300 футов.

Вопрос. Какие уровни мощности передачи доступны для точки доступа 1200?

Ответ. Параметры мощности передачи различаются в зависимости от используемых радиомодулей. См. полный список уровней мощности в документе Точка доступа Cisco Aironet 1200. 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 разрешить подключение к точке доступа только для клиентов 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.

Ответ. Чтобы разрешить точке доступа принимать только клиенты 802.11g, выполните следующие действия в графическом интерфейсе:

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:
 - 1.0
 - 2.0
 - 5.5
 - 11.0
6. Выберите **Require** для всех остальных скоростей передачи данных. Эти скорости:
 - 6.0
 - 9.0
 - 12.0
 - 18.0
 - 24.0
 - 36.0
 - 48.0
 - 54.0
9. Нажмите кнопку **Apply** в нижней части окна. Пример настройки представлен на следующем окне:

Data Rates:	Best Range	Best Throughput	Default
1.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
2.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
5.5Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
* 6.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 9.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
11.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
* 12.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 18.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 24.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 36.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 48.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 54.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable

* OFDM Rates

10.

Вопрос. Правда ли, что если я разрешу подключение к беспроводной сети только для клиентов IEEE 802.11g, они не смогут вызывать помехи в параллельной сети IEEE 802.11b, так как эти клиенты используют разные схемы модуляции?

Ответ. Нет, это не правда. 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 Ethernet-порта точки доступа?

Ответ. Ethernet-порт точки доступа поддерживает скорости 10 Мбит/с и 100 Мбит/с через разъем RJ-45 в полудуплексном или дуплексном режимах. Необходимо зафиксировать параметры скорости и дуплекса, аналогичные параметрам коммутатора или концентратора.

Вопрос. Каковы возможные источники помех для радиочастотного канала связи точки доступа?

Ответ. Помехи могут вызывать различные источники, в том числе:

- 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.

- Устранение неисправностей, влияющих на радиочастотную связь
- Проблемы пропадающего подключения в беспроводных мостах

Вопрос. Как вернуть точку доступа к заводским параметрам по умолчанию?

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

Вопрос. Могут ли продукты серий 340, 350, 1100 и 1300 взаимодействовать друг с другом?

Ответ. Да, если эти продукты работают на одной частоте, они полностью совместимы:

- 340
- 350
- 1100 (с радиомодулем 2,4 ГГц)
- 1200 и 1300 (с радиомодулем 2,4 ГГц)

Модель 1200 с дополнительным радиомодулем IEEE 802.11a 5 ГГц несовместима с продуктами IEEE 802.11b. Все продукты Aironet соответствуют стандарту Wi-Fi и должны быть совместимы с продуктами других производителей, которые также соответствуют этому стандарту.

Вопрос. Каковы основные различия между точками доступа серий 340 и 350?

Ответ. Основные различия между линейками продуктов связаны с мощностью радиомодулей, а также с поддержкой модульной структуры, позволяющей обновлять системы в будущем. Модели 350, 1100 и 1200 имеют более мощные радиомодули IEEE 802.11b. Их мощность составляет 100 мВт. Модели 340 имеют радиомодуль 802.11b мощностью 30 мВт. Модели 1200 имеют модульный слот, в который можно установить радиомодуль IEEE 802.11a. Радиомодули 1100 и 1200 802.11b производятся в форм-факторе mini-PCI (mini-Peripheral Component Interconnect), что позволяет модернизировать радиомодули с выходом новых продуктов.

Примечание: Производство точек доступа 340 прекращено и их невозможно купить.

Вопрос. Почему клиентская плата не соединяется с ближайшей точкой доступа?

Ответ. Если в вашей беспроводной топологии присутствует несколько точек доступа, клиент будет поддерживать соединение с точкой доступа, с которой он был соединен первоначально, до тех пор, пока не прекратит принимать сигналы маяки Keeralive от этой точки доступа. 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. Поддерживается ли в точках доступа механизм аварийного переключения или избыточность?

Ответ. Да. Да, можно настроить "горячее" резервирование для обеспечения избыточности на случай отказа основной точки доступа. Дополнительные сведения см. в разделе *Дополнительные этапы установки "горячего" резервирования* документа Заметки о выпуске для точек доступа Cisco Aironet.

Вопрос. Что такое WEP-ключ?

Ответ. Аббревиатура WEP расшифровывается как Wired Equivalent Privacy (эквивалент секретности проводной сети). 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. дополнительные сведения о настройке WEP в документе Настройка WEP (Wired Equivalent Privacy).

Вопрос. Какой порт необходимо указать для связи с сервером Cisco ACS, при использовании протокола LEAP?

Ответ. По умолчанию сервер ACS слушает запросы на аутентификацию через порт 1645 и выполняет учет на порте 1646. Однако, можно настроить порт 1812 для аутентификации и порт 1813 для учета. Убедитесь, что эти порты корректно заданы на странице "Authentication Server Setup" точки доступа.

Вопрос. У меня есть точка доступа Cisco и сервер ACS версии 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." Почему точка доступа выдает эти сообщения об ошибке?

Ответ. Одна из возможных причин этих сообщений об ошибке — разные общие ключи на точке доступа и сервере 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. Дополнительные сведения об отладке см. в документе Отладка аутентификации.

Вопрос. При просмотре журналов точки доступа была обнаружена следующая ошибка. "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." Какова причина этой ошибки и как решить проблему?

Ответ. Появление этой ошибки в журнале вполне обычно, если на точке доступа настроен параметр **radius-server deadtime**. 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 не отвечающими 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. Я использую точку доступа 1230 с ПО Cisco IOS версии 12.3(4)JO. При обновлении списка контроля доступа ACL появляется следующее сообщение "% Warning: Saving this config to nvram may corrupt any network management or security files stored at the end of nvram. Continue? [no]:"

Ответ. Это предупреждающее сообщение, а не ошибка. Если вы выберете [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 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: Введите команду **delete flash:** для каждого RCORE-файла во Flash-памяти.

Вопрос. Я использую модуль WLSM с ПО Cisco IOS версии 12.4(4)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?

Ответ. Оба сообщения указывают на проблему РЧ. Чтобы устранить проблему, назначьте точке доступа другие каналы.

Вопрос. Можно ли использовать статические ключи WEP и протокол EAP для аутентификации на одной точке доступа? Это было возможно в точках доступа на базе VxWorks.

Ответ. Нет, использовать статические ключи WEP для шифрования и протокол EAP для аутентификации на одном SSID нельзя. ПО VxWorks позволяло создавать такую конфигурацию из-за программной уязвимости. Но эта возможность 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. Обследование узла действительно необходимо?

Ответ. 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 изменить конфигурацию точки доступа запрашивается пароль. Что необходимо ввести?

Ответ. Предложение ввести имя пользователя и пароль говорит о том, что включена функция User Manager. 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 антенны для покрытия двух сот (например, антенну 1 для соты 1 и антенну 2 для соты 2)?

Ответ. Использовать две антенны на точке доступа для покрытия двух сот нельзя. 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. Для чего используется команда "mobility network-id" точки доступа?

Ответ. Команда **mobility network-id** используется для настройки мобильной сети уровня 3 в рамках 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. Неправильное использование команды может привести к возникновению следующих проблем подключения:

- клиенты не получают IP-адреса от DHCP.
- в некоторых случаях, клиенты не могут соединиться с точкой доступа.
- беспроводные клиенты не могут соединиться 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 SSID можно настроить для каждой сети VLAN?

Ответ. В сети VLAN можно настроить только один идентификатор SSID. Использование нескольких идентификаторов SSID в одной сети VLAN в точках доступа Aironet не поддерживается.

Вопрос. Точки доступа Cisco Aironet в сети WLAN не рассылают идентификаторы SSID. Почему? Нужно ли включить определенную функцию в точке доступа?

Ответ. Если вы не включили гостевой режим в приложении SSID Manager, точка доступа не будет рассылать идентификаторы SSID в 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. Я использую точку доступа 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?

Ответ. Точка доступа AIR-AP1231G-A-K9 AP имеет радиомодуль 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. Можно ли настроить радиомодуль А в качестве моста и радиомодуль G в качестве точки доступа? Если да, то как?

Ответ. Да, каждый радиомодуль в точке доступа можно настроить на выполнение разных функций. В вашем сценарии это можно сделать, установив разные идентификаторы SSID для радиомодулей G и A. Затем установите следующие роли в радиосети, точка доступа (AP) для радиомодуля G и корневой мост (root bridge) для радиомодуля A.

Вопрос. Я использую точку доступа 1100. 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.

Ответ. Обновление радиомодуля 802.11b до 802.11g не приведет к улучшению производительности, если вы продолжите использовать клиенты 802.11b. 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. Когда два клиента соединяются с двумя разными точками доступа, которые подключены к одной подсети, они будут связаны через проводной или через беспроводной канал?

Ответ. В этом сценарии, если две точки доступа работают в режиме root, связь между ними будет осуществляться 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 включить маршрутизацию или преобразование сетевых адресов (NAT) на точках доступа Cisco?

Ответ. Нет. Функции NAT и маршрутизации не поддерживаются на точках доступа.

Вопрос. Если ли способ создать расписание доступности точки доступа на базе Cisco IOS? Я хотел бы предоставить доступ на основе времени суток клиентам, которые подключаются к точке доступа.

Ответ. Доступ на основе времени суток можно настроить, добавив временные интервалы в списки контроля доступа ACL.

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. Могут ли точки доступа использовать несколько DHCP-пулов в разных подсетях?

Ответ. При настройке точки доступа в качестве DHCP-сервера, IP-адреса назначаются устройствам, которые находятся в одной подсети с DHCP-сервером. 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 качестве DHCP-сервера.

Вопрос. Я использую беспроводной IP-телефон Cisco 7920, подключенный к точке доступа Cisco. IP-телефон 7920 соединяется с точкой доступа, но IP-адрес не назначается. Я использую протокол EAP. Появляются сообщения "Info Station [SEP001121ceb9a4]001121ceb9a4 Authenticated", "Info Station [SEP001121ceb9a4]001121ceb9a4 Reassociated" и "Warning EAP retry limit reached for Station [SEP001121ceb9a4]001121ceb9a4". После этого отображается сообщение "Info Deauthenticating [SEP001121ceb9a4]001121ceb9a4, reason 'Previous Authentication No Longer Valid' ". В чем проблема?

Ответ. Причина появления этих сообщений в том, что общий секрет точки доступа отличается от общего секрета сервера RADIUS. Убедитесь, что общие секреты для аутентификации EAP одинаковы. Повторно введите общий секрет на точке доступа и сервере RADIUS.

Вопрос. В чем смысл показателя дБм? Как определить эквивалентные значения дБм для уровня сигнала (в мВт), который отображается для точки доступа Aironet?

Ответ. Уровень сигнала измеряется в децибелах (дБ), как отношение уровня к другому стандартному 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:

$$\text{Мощность (в дБ)} = 10 * \log_{10} (\text{сигнал/эталон})$$

В этом списке объясняются значения формулы. \log_{10} — это десятичный логарифм.

- Сигнал — это мощность сигнала (например, 50 мВт).
- Эталон — это эталонное значение мощности (например, 1 мВт)

Пример:

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

$$\text{Power (in dB)} = 10 * \log_{10} (50/1) = 10 * \log_{10} (50) = 10 * 1.7 = 17 \text{ dBm}$$

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:

dBm	mW
0	1
1	1.25
2	1.56
3	2
4	2.5
5	3.12
6	4
7	5
8	6.25
9	8
10	10
11	12.5
12	16
13	20
14	25
15	32
16	40
17	50
18	64
19	80
20	100
21	128
22	160
23	200
24	256
25	320
26	400
27	512
28	640
29	800
30	1000 or 1 W

См. дополнительные сведения в документе Значения мощности РЧ.

Вопрос. Проблема с точкой доступа. 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?

Ответ. Да, такое поведение считается штатным. 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. Как изменить параметры даты и времени на точке доступа Cisco 1231?

Ответ. Откройте web-интерфейс (GUI) и выберите **Services > SNTP**, затем выберите **Time Settings** и измените время.

Вопрос. Мы используем беспроводные точки доступа Cisco LWAPP. 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?

Ответ. Количество поврежденных и повторно отправленных пакетов — две основные метрики сети 802.11 WLAN. Анализ поврежденных и повторно отправленных пакетов в 802.11 отличается 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 означает, 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. Если функция ССКМ НЕ настроена клиенте, но настроена на точке доступа, смогут ли клиенты соединиться с этой точкой доступа? Смогут ли клиенты выполнять нормальный роуминг?

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

В зависимости от развертываемых клиентов, рекомендуется устанавливать функцию ССКМ на режим "optional" в инфраструктуре, которая разрешает соединение со всеми устройствами, но поддерживает роуминг ТОЛЬКО для устройств, соединенных с использованием ССКМ.

Вопрос. Какова разница в объеме памяти между точками доступа 1240 и 1230?

Ответ. Объемы памяти точке доступа 1240 и 1230:

- 1240 — это точка доступа с платформой 32 МБ;
- 1230 — это точка доступа с платформой 16 МБ.

Вопрос. Я использую две точки доступа 1240 с поддержкой гибких ролей. 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?

Ответ. Гибкие роли точки доступа поддерживают режим моста для точек доступа, которые могут работать в двух диапазонах (1200, 1230 и 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. Какое количество беспроводных IP-телефонов рекомендуется на одну точку доступа?

Ответ. Определение размера сети IP-телефонии необходимо для гарантии доступности пропускной способности и ресурсов, которые требуются для переноса критического 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 рассмотрением 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. Большой 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 настроить точку доступа 1200 на прекращение обработки запросов на аутентификацию после определенного числа попыток?

Ответ. Для ограничения числа попыток клиентов получить доступ к сети можно использовать параметр "maximum retries" сервера AAA. Значение этого параметра можно настроить вручную на сервере AAA или использовать количество попыток по умолчанию, которое зависит от используемого сервера AAA.

Вопрос. Где можно найти информацию о различиях платформ AP (точка доступа) и LAP (облегченная точка доступа).

Ответ. См. документ Обзор решения — беспроводные точки Cisco Aironet. Он содержит данные о сравнении различных моделей обычных точек доступа и точек доступа LAP.

Вопрос. Поддерживается ли в точках доступа Cisco Aironet функция PPPoE?

Ответ. Нет. Функция PPPoE не поддерживается в точках доступа Cisco Aironet.

Вопрос. Поддерживается ли в точках доступа Cisco Aironet протокол VTP?

Ответ. Нет. Протокол VTP не поддерживается в точках доступа Cisco Aironet.

Дополнительные сведения

- [Загружаемые файлы для беспроводных продуктов Cisco](#)
- [Cisco Aironet 1240 AG Series Q&A](#)
- [Cisco Aironet 1230 AG Series Q&A](#)
- [Руководство по конфигурации программного обеспечения VxWorks для точек доступа Cisco Aironet](#)
- [Руководство по конфигурации программного обеспечения IOS для точек доступа Cisco Aironet](#)
- [Ресурсы поддержки беспроводных систем](#)
- [Примечания об устранении неполадок Cisco Aironet 350](#)
- [Страница поддержки беспроводных систем](#)
- [Техническая поддержка и документация — Cisco Systems](#)

© 1992-2010 Cisco Systems, Inc. Все права защищены.

Дата генерации PDF файла: Jan 05, 2010

<http://www.cisco.com/support/RU/customer/content/9/97417/ap-faq.shtml>
