Пример настройки типов аутентификации на фиксированном ISR с помощью SDM

Содержание

Введение

Этот документ предоставляет примеры конфигурации, которые объясняют, как настроить различные типы проверки подлинности Уровня 2 на интегрированном маршрутизаторе фиксированной конфигурации беспроводной связи Cisco для возможности беспроводного подключения с программой Security Device Manager (SDM).

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Знание того, как настроить основные параметры Cisco ISR (ISR) с SDM
- Знание того, как настроить 802.11a/b/g адаптер беспроводного клиента со служебной программой рабочего стола Aironet (ADU)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Маршрутизатор Cisco 877W ISR использующий программное обеспечение Cisco IOS® версии 12.3(8)YI1
- Версия 2.4.1 SDM Cisco установлена на ISR
- Портативный ПК с версией 3.6 служебной программы рабочего стола Aironet
- Клиентский адаптер a/b/g 802.11, который выполняет Версию микропрограммы 3.6

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

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

Общие сведения

SDM Cisco является интуитивным, находящимся на web программным средством управления устройствами для маршрутизаторов на основе ПО Cisco IOS. SDM Cisco упрощает маршрутизатор и конфигурацию безопасности через умных мастеров, которые помогают клиентам быстро и легко развертывают, настраивают и контролируют маршрутизаторы Cisco Systems®, не требуя знания интерфейса командной строки (CLI) программного обеспечения Cisco IOS.

SDM может быть загружен бесплатно от Центра программного обеспечения на Cisco.com.

SDM может быть установлен независимо как отдельная копия на каждом отдельные маршрутизаторы, или он может также быть установлен на ПК. SDM Cisco, установленный на ПК, позволяет вам использовать SDM для управления другими маршрутизаторами, которые выполняют надлежащие Образы IOS в сети. Однако SDM на ПК не поддерживает сброс конфигурации маршрутизатора для Производства по умолчанию.

Этот документ использует SDM, установленный на беспроводном маршрутизаторе для настройки маршрутизатора для беспроводной аутентификации.

SDM Cisco связывается с маршрутизаторами в двух целях:

- Обратитесь к файлам приложения SDM Cisco для загрузки к ПК
- Считайте и запишите конфигурацию маршрутизатора и статус

SDM Cisco использует HTTP для загрузки файлов приложения (sdm.tar, home.tar) к ПК. Комбинация HTTP и Telnet/SSH используется, чтобы считать и записать конфигурацию маршрутизатора.

См. Вопросы и ответы Cisco Router and Security Device Manager для последней информации о маршрутизаторах и выпусках ПО IOS тот SDM поддержки.

См. Настраивают Ваш маршрутизатор для Поддержки SDM для получения дополнительной информации о том, как использовать SDM Cisco на маршрутизаторе.

См. Установку Файлы SDM для инструкций, чтобы установить и загрузить файлы SDM на маршрутизаторе или на ПК.

Настройка

Документ объясняет, как настроить эти типы проверки подлинности через SDM:

- Открытая аутентификация с шифрованием WEP
- Открытый с проверкой подлинности MAC
- Совместно используемая аутентификация
- Аутентификация 802.1x/протокола EAP
- Защищенный доступ по протоколу Wi-Fi (WAP) - аутентификация Пред общего ключа (PSK)
- Аутентификация WPA

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:

Эта настройка использует локальный сервер RADIUS на беспроводном ISR для аутентификации беспроводных клиентов, использующих аутентификацию 802.1x.

Настройте маршрутизатор для доступа SDM

Выполните эти шаги, чтобы позволить маршрутизатору быть обращенным через SDM:

1. Настройте маршрутизатор для доступа http/https с помощью процедуры, объясненной в, Настраивают маршрутизатор для Поддержки SDM.
2. Назначьте IP-адрес на маршрутизатор с этими шагами:`Router#`**`configure terminal`** `Enter configuration commands, one per line. End with CNTL/Z. Router(config)#`**`interface fastEthernet 0`** `Router(config-if)#`**`ip address`***`10.77.244.197 255.255.255.224`* **`% IP addresses`**

`cannot be configured on L2 links.` В маршрутизаторе на 871 Вт вы могли бы встретиться с таким сообщением об ошибках. Это сообщение об ошибках показывает, что Fast Ethernet 0 является ссылкой Уровня 2, на которой вы не можете настроить IP-адрес.
3. Для преодоления этой проблемы создайте Уровень 3 (VLAN), взаимодействуют и назначают IP-адрес на том же с этими шагами:`Router(config)#interface Vlan1 Router(config-if)#ip address 10.77.244.197 255.255.255.224`
4. Позвольте эту VLAN на Fast Ethernet Уровня 2 0 интерфейсов с этими шагами. Этот документ настраивает интерфейс Fast Ethernet как интерфейс магистрали для разрешения VLAN1. Можно также настроить его как интерфейс доступа и позволить VLAN1 на интерфейсе на сетевую установку.`Router(config)#interface fastEthernet 0 Router(config-if)#switchport trunk encapsulation dot1q Router(config-if)#switchport trunk allowed vlan add vlan1 !--- This command allows VLAN1 through the fast ethernet interface. !--- In order to allow all VLANs through this interface, issue the !--- switchport trunk allowed vlan add all command on this interface.` **Примечание:** Данный пример предполагает, что основной маршрутизатор и конфигурации беспроводной сети уже выполнены на маршрутизаторе. Поэтому следующий шаг должен немедленно запустить приложение беспроводной связи на маршрутизаторе для настройки параметров аутентификации.

Запустите приложение беспроводной связи SDM на маршрутизаторе

Выполните эти шаги для запуска приложения беспроводной связи:

1. Запустите SDM путем открытия браузера и ввода IP-адреса маршрутизатора.Вам предлагают принять или уменьшить окно Web Browser Security Alert, которое похоже на это:
2. Нажмите **Yes** для перехода.
3. На окне, которое появляется, введите привилегию level_15 имя пользователя и пароль для доступа к маршрутизатору.Данный пример использует **admin** в качестве имени пользователя и пароля:
4. **Для продолжения нажмите кнопку OK.** Введите ту же информацию везде, где она требуется.
5. Нажмите **Yes** и **OK** как соответствующие на результирующих страницах для запуска приложения SDM.Когда приложение SDM открывается, вам предлагает окно сигнала о нарушении безопасности принять сертификат безопасности со знаком.
6. Нажмите **Yes** для принятия подписанного сертификата.Результирующий маршрутизатор Cisco и главная страница SDM похожи на это:
7. На этой странице нажмите **Configure** наверху для запуска окна режима конфигурации маршрутизатора.
8. В окне режима конфигурации выберите **Interfaces и Connections** от столбца Tasks, который появляется в левой части этой страницы.
9. В окне Interfaces и Connections нажмите вкладку **Create Connection**.Это перечисляет все интерфейсы, доступные, чтобы быть настроенным на маршрутизаторе.
10. Для запуска приложения беспроводной связи выберите **Wireless** из списка интерфейсов. Затем нажмите **Launch Wireless Application**.Этот снимок экрана объясняет шаги 8, 9 и 10:Это запускает Приложение беспроводной связи SDM в отдельном окне, где могут быть настроены различные типы проверки подлинности.Домашняя страница Приложения беспроводной связи SDM похожа на это:Заметьте, что Состояние ПО **Отключено**, и Состояние оборудования радио-

(беспроводного) интерфейса **не работает**, потому что никакой SSID не настроен на интерфейсе. Затем, вы настраиваете SSIDs и типы проверки подлинности на этом радиоинтерфейсе так, чтобы беспроводные клиенты могли связаться через этот интерфейс.

Настройте открытую аутентификацию с шифрованием WEP

Открытая аутентификация является алгоритмом фиктивной проверки подлинности. Точка доступа (AP) предоставит любой запрос об аутентификации. Открытая аутентификация позволяет любой доступ к сети устройства. Если никакое шифрование не включено в сети, никакое устройство, которое знает, SSID AP может получить доступ к сети. С Шифрованием WEP, включенным на AP, сам Ключ WEP становится средством управления доступом. Если устройство не будет иметь корректного Ключа WEP, даже при том, что аутентификация успешна, то устройство будет неспособно передать данные через AP. Кроме того, это не может дешифровать данные, передаваемые от AP.

См. Открытую аутентификацию к точке доступа для получения дополнительной информации.

Данный пример использует эти параметры конфигурации для открытой аутентификации с Шифрованием WEP:

- Название SSID: **openwep**
- Идентификатор VLAN: **1**
- IP-адрес VLAN: **10.1.1.1/16**
- Диапазон адресов DHCP для беспроводных клиентов этой VLAN/SSID: **10.1.1.5/16 - 10.1.1.10/16**

Выполните эти шаги для настройки открытой аутентификации с WEP:

1. На домашней странице Приложения беспроводной связи нажмите **Wireless Services> VLAN** для настройки VLAN.
2. Выберите **Routing** от Сервисов: страница VLAN.
3. На Сервисах: страница VLAN Routing, создайте VLAN и назначьте его на радиоинтерфейс.Это - окно конфигурации VLAN1 на радиоинтерфейсе. VLAN1 является собственным VLAN здесь:
4. На домашней странице Приложения беспроводной связи выберите **Wireless Security> SSID Manager** для настройки SSID и типа проверки подлинности.
5. На Безопасности: страница SSID Manager, настройте SSID и назначьте SSID на VLAN, созданную в step1 для включения SSID на радиоинтерфейсе.
6. Под разделом параметров аутентификации этой страницы выберите **Open Authentication**.Вот окно конфигурации, которое объясняет эти шаги:
7. **Щелкните "Применить".Примечание:** Раскрывающееся окно, которое соответствует Флажку открытой аутентификации, подразумевает, что открытая аутентификация может быть настроена, кроме того, с несколькими дополнительными типами проверки подлинности, такими как EAP или проверка подлинности MAC. В этом разделе рассматриваются только открытую аутентификацию без ДОБАВЛЕНИЯ (без дополнительного типа проверки подлинности).
8. Настройте Шифрование WEP для этого SSID/VLAN. На беспроводной домашней странице выберите **Wireless Security> Encryption Manager** для настройки настроек

шифрования.На Безопасности: страница Encryption Manager, набор Режим шифрования и Ключи для **VLAN1**.Выберите **WEP Encryption: обязательный** как режим шифрования.Установите Ключ шифрования для этой VLAN.Этот раздел использует эти параметры настройки ключа шифрования:Слот Encryption key 1: используемый в качестве Ключа передачиРазмер ключа шифрования: 40 битовКлюч шифрования в шестнадцатеричном значении: 1234567890**Примечание:** Тот же слот encryption key (1, в этом случае) должен использоваться в качестве ключа передачи в беспроводном клиенте. Кроме того, беспроводной клиент должен быть настроен с тем же значением параметра (1234567890 в этом случае) для беспроводного клиента для передачи с этой сетью WLAN.Это окно конфигурации объясняет эти шаги:Эта страница Wireless Security представляет полную конфигурацию:

Настройте внутренний сервер DHCP для беспроводных клиентов этой VLAN

Выполните эти шаги для настройки внутреннего сервера DHCP на маршрутизаторе. Это - дополнительное, хотя рекомендуется, метод для присвоения IP-адреса на беспроводных клиентов.

1. На окне режима конфигурации SDM выберите **Additional Tasks** под столбцом Tasks, который находится на левой части окна.
2. На странице **Additional Tasks** разверните дерево **DHCP** и выберите **DHCP Pools** как показано в данном примере. В столбце DHCP Pools, показанном на правой части этой страницы**, нажмите Add** для создания нового пула DHCP.
3. На странице Add DHCP Pool задайте Название ПУЛА DHCP, Сеть ПУЛА DHCP, Маску подсети, Запустив IP-адрес, Закончив параметры IP-адреса и Маршрутизатора по умолчанию как показано в данном примере:
4. **Нажмите кнопку ОК.**Внутренний сервер DHCP настроен на маршрутизаторе.

Настройте открытый с проверкой подлинности MAC

В этом типе аутентификации беспроводному клиенту разрешат обратиться к сети WLAN, только если MAC-адрес клиента находится под списком разрешенных адресов MAC в сервере проверки подлинности. AP передает MAC-адрес беспроводного клиентского устройства к Серверу проверки подлинности RADIUS в вашей сети, и сервер проверяет адрес против списка разрешенных адресов MAC. На основе MAC аутентификация предоставляет альтернативный метод аутентификации для устройств клиента, которые не имеют возможности EAP.

См. Аутентификацию с использованием MAC-адреса к Сети для получения дополнительной информации.

Примечание: Весь документ использует локальный сервер RADIUS для проверки подлинности MAC, 802.1x/EAP, а также аутентификации WPA.

Данный пример использует эти параметры конфигурации для открытого с проверкой подлинности MAC:

- Название SSID: **openmac**
- Идентификатор VLAN: **2**

- IP-адрес VLAN: **10.2.1.1/16**
- Диапазон адресов DHCP для беспроводных клиентов этой VLAN/SSID: **10.2.1.5/16 - 10.2.1.10/16**

Выполните эти шаги для настройки открытый с проверкой подлинности MAC:

1. На домашней странице Приложения беспроводной связи нажмите **Wireless Services> VLAN** для настройки VLAN.
2. Выберите **Routing** от Сервисов: страница VLAN. На Сервисах: страница VLAN Routing, создайте VLAN и назначьте его на радиоинтерфейс.Вот окно конфигурации **VLAN 2** на радиоинтерфейсе:
3. Настройте локальный сервер RADIUS для проверки подлинности MAC. Этот локальный сервер RADIUS будет держать MAC-адрес беспроводного клиента в его базе данных и разрешит или запретит клиента в сеть WLAN согласно результату аутентификации.На беспроводной домашней странице выберите **Wireless Security> Server Manager** для настройки локального сервера RADIUS.На странице Server Manager настройте IP-адрес, Общий секретный ключ, и Аутентификацию и Порты учета сервера RADIUS.Поскольку это - локальный сервер RADIUS, заданный IP-адрес является адресом этого беспроводного интерфейса. Используемый общий секретный ключ должен быть тем же на конфигурации клиента AAA.В данном примере общий секретный ключ является **Cisco**.**Щелкните "Применить".**Прокрутите страницу вниз для поиска раздела Приоритетов Сервера По умолчанию. В этом разделе выберите этот сервер RADIUS **(10.2.1.1)** в качестве сервера приоритета по умолчанию для Проверки подлинности MAC как показано в данном примере:Для настройки клиента AAA и учетных данных пользователя, выберите **Wireless Security> Local RADIUS Server** от беспроводной домашней страницы.На странице Local RADIUS Server нажмите **GENERAL SET-UP**.На ОБЩЕЙ Странице настройки настройте клиента AAA и общий секретный ключ как показано.С конфигурацией локального сервера RADIUS IP-адрес сервера и клиента AAA будет тем же.Прокрутите ОБЩУЮ СТРАНИЦУ НАСТРОЙКИ ВНИЗ для поиска раздела конфигурации **Отдельных пользователей**. В разделе Отдельных пользователей настройте MAC-адрес беспроводного клиента как имя пользователя и пароль.Включите флажок **MAC Authentication Only**, затем нажмите **Apply**.Во избежание клиента от ошибки проверки подлинности время от времени, задайте MAC-адрес клиента в непрерывном формате без любого разделения как показано в данном примере.
4. На домашней странице Приложения беспроводной связи выберите **Wireless Security> SSID Manager** для настройки SSID и типа проверки подлинности.На Безопасности: страница SSID Manager, настройте SSID и назначьте SSID на VLAN, созданную в step1 для включения SSID на радиоинтерфейсе.Под разделом параметров аутентификации этой страницы выберите **Open Authentication** и из соответствующего раскрывающегося окна, выберите **с Проверкой подлинности MAC**.Для настройки Приоритетов Сервера выберите**, Customize** под MAC Аутентифицируют Серверы и выбирают IP-адрес локального сервера RADIUS **10.2.1.1**.Это - пример, который объясняет этот шаг:
5. Для настройки внутреннего сервера DHCP для беспроводных клиентов этой VLAN выполните те же шаги, объясненные в Настраивать Внутреннем сервере DHCP для Беспроводных клиентов Этого раздела VLAN этого документа с этими параметрами конфигурации:Название ПУЛА DHCP: VLAN 2Сеть ПУЛА DHCP: 10.2.0.0Маска подсети: 255.255.0.0Стартовый IP: 10.2.1.5Конечный IP: 10.2.1.10Маршрутизатор по умолчанию: 10.2.1.1

Настройте 802.1X/АУТЕНТИФИКАЦИЮ EAP

Этот тип проверки подлинности предоставляет высший уровень безопасности для вашей беспроводной сети. При помощи EAP для взаимодействия с совместимым с EAP сервером RADIUS AP помогает беспроводному клиентскому устройству и серверу RADIUS выполнять обоюдную проверку подлинности и получать динамический Ключ WEP индивидуальной рассылки. Сервер RADIUS передает Ключ WEP к AP, который использует его для всех сигналов многоадресных данных, что это передает к или получает от клиента.

См. Аутентификацию eap к Сети для получения дополнительной информации.

Примечание: Существует несколько методов доступной Аутентификации eap. Всюду по этому документу это объясняет, как настроить Легковесный расширяемый протокол аутентификации (LEAP) как Аутентификацию eap. LEAP использует имя пользователя и пароль в качестве учетных данных пользователя для аутентификации.

Примечание: Для настройки Гибкой аутентификации EAP через Безопасный, Туннелирующий (EAP-FAST) как тип Аутентификации eap, обратитесь к Руководству по конфигурации Версии 1.02 EAP-FAST для процедуры.

Данный пример использует эти параметры конфигурации для Аутентификации eap:

- Название SSID: **скачок**
- Идентификатор VLAN: **3**
- IP-адрес VLAN: **10.3.1.1/16**
- Диапазон адресов DHCP для беспроводных клиентов этой VLAN/SSID: **10.3.1.5/16 - 10.3.1.10/16**

Выполните эти шаги для настройки Аутентификации eap:

1. Повторите, что шаги 1 и 2 Настраивают Открытый с Проверкой подлинности MAC, чтобы создать и настроить VLAN с этими параметрами конфигурации:Идентификатор VLAN: 3IP-адрес радиоинтерфейса: 10.3.1.1маска подсети: 255.255.0.0
2. Затем настройте локальный сервер RADIUS для аутентификации клиента. Для выполнения этого повторите, что шаги 3a к 3c Настраивают Открытый с Проверкой подлинности MAC с этими параметрами конфигурации:IP-адрес сервера RADIUS: 10.3.1.1Общий secret: ciscoВот окно конфигурации, которое объясняет шаг 2 Аутентификации eap:
3. Прокрутите страницу вниз для поиска раздела Приоритетов Сервера По умолчанию. В этом разделе выберите этот сервер RADIUS **(10.3.1.1)** в качестве сервера приоритета по умолчанию для Аутентификации eap как показано в данном примере.
4. Повторите, что шаги 3e и 3f Настраивают Открытый с Проверкой подлинности MAC.
5. Повторите, что шаги 3g и 3 h Настраивают Открытый с Проверкой подлинности MAC с этими параметрами конфигурации для Аутентификации eap:IP-адрес клиента AAA: 10.3.1.1Общий secret: ciscoПод разделом Отдельных пользователей настройте имя пользователя и пароль как **user1**.
6. На домашней странице Приложения беспроводной связи выберите **Wireless Security> SSID Manager** для настройки SSID и типа проверки подлинности.На Безопасности: страница SSID Manager, настройте SSID и назначьте SSID на VLAN, созданную в шаге 1 для включения SSID на радиоинтерфейсе.Под разделом параметров аутентификации этой страницы выберите **Open Authentication** и из соответствующего

раскрывающегося окна, выберите **EAP Authentication**. Кроме того, выберите **Сетевой** тип **Аутентификации eap**.Для настройки Приоритетов Сервера выберите**, Customize** под EAP Аутентифицируют Серверы и выбирают IP-адрес локального сервера RADIUS **10.3.1.1**.Вот пример, который объясняет эти шаги:

7. Для настройки внутреннего сервера DHCP для беспроводных клиентов этой VLAN выполните те же шаги, объясненные в Настраивать Внутреннем сервере DHCP для Беспроводных клиентов Этого раздела VLAN этого документа с этими параметрами конфигурации:Название ПУЛА DHCP: VLAN 3Сеть ПУЛА DHCP: 10.3.0.0Маска подсети: 255.255.0.0Стартовый IP: 10.3.1.5Конечный IP: 10.3.1.10Маршрутизатор по умолчанию: 10.3.1.1
8. Настройте Шифр, который будет использоваться для управления динамического ключа после успешной аутентификации беспроводного клиента.На беспроводной домашней странице выберите **Wireless Security> Encryption Manager** для настройки настроек шифрования.На экране Wireless Security> Encryption Manager на Безопасности: страница Encryption Manager, войдите **3** для Режима шифрования Набора и Ключей для VLAN.Выберите **Cipher** в качестве Режима шифрования и выберите алгоритм шифрования Cipher из раскрывающегося окна.Данный пример использует **TKIP** в качестве алгоритма Шифра:**Примечание:** В то время как настройка несколько серверов проверок подлинности вводит на беспроводном маршрутизаторе через SDM, иногда не могло бы быть возможно настроить два других типа проверки подлинности оба режима шифрования шифра использования на том же маршрутизатор. В таких случаях настройка шифрования, настроенная через SDM, не могла бы быть применена на маршрутизатор. Для преодоления этого настройте те типы проверки подлинности через CLI.

Настройте совместно используемую аутентификацию

Cisco предоставляет проверку подлинности с общим ключом для соответствия стандарту IEEE 802.11b.

Во время проверки подлинности с общим ключом AP передает незашифрованную строку текста запроса к любому устройству, которое пытается связаться с AP. Устройство, которое запрашивает аутентификацию, шифрует текст запроса и передает ее обратно в AP. Если текст запроса зашифрован правильно, AP позволяет запрашивающему устройству аутентифицироваться. И незашифрованная проблема и зашифрованная проблема могут быть проверены. Однако это оставляет AP открытым для нападения от злоумышленника, который вычисляет Ключ WEP путем сравнения незашифрованных и зашифрованных текстовых строк.

См. Проверку подлинности с общим ключом к точке доступа для получения дополнительной информации.

Данный пример использует эти параметры конфигурации для совместно используемой аутентификации:

- Название SSID: **совместно используемый**
- Идентификатор VLAN: **4**
- IP-адрес VLAN: **10.4.1.1/16**
- Диапазон адресов DHCP для Беспроводных клиентов этой VLAN/SSID: **10.4.1.5/16 -**

10.4.1.10/16

Выполните эти шаги для настройки совместно используемой аутентификации:

1. Повторите, что шаги 1 и 2 Настраивают Открытый с Проверкой подлинности MAC, чтобы создать и настроить VLAN с этими параметрами конфигурации:Идентификатор VLAN: 4IP-адрес радиоинтерфейса: 10.4.1.1маска подсети: 255.255.0.0
2. На домашней странице Приложения беспроводной связи выберите **Wireless Security> SSID Manager** для настройки SSID и типа проверки подлинности.На Безопасности: страница SSID Manager, настройте SSID и назначьте SSID на VLAN, созданную в step1 для включения SSID на радиоинтерфейсе.Под разделом параметров аутентификации этой страницы выберите **Shared Authentication**.Вот окно конфигурации, которое объясняет эти шаги:**Щелкните "Применить".**
3. Настройте Шифрование WEP для этого SSID/VLAN. Поскольку это - проверка подлинности с общим ключом, тот же ключ используется для аутентификации также. На беспроводной домашней странице выберите **Wireless Security> Encryption Manager** для настройки настроек шифрования.На Безопасности: страница Encryption Manager, войдите **4** для Режима шифрования Набора и Ключей для VLAN.Выберите **WEP Encryption: обязательный** как режим шифрования.Установите Ключ шифрования для этой VLAN.Этот раздел использует эти параметры настройки ключа шифрования:Слот Encryption Key 1: используемый в качестве Ключа передачиРазмер Ключа шифрования: 40 битовКлюч шифрования в шестнадцатеричном значении: 1234567890**Примечание:** Тот же слот encryption key (1, в этом случае) должен использоваться в качестве ключа передачи в беспроводном клиенте. Кроме того, беспроводной клиент должен быть настроен с тем же значением параметра (1234567890 в этом случае) для беспроводного клиента для передачи с этой сетью WLAN.Это окно конфигурации объясняет эти шаги:
4. Для настройки внутреннего сервера DHCP для беспроводных клиентов этой VLAN выполните те же шаги, объясненные в, Настраивают Внутренний сервер DHCP для Беспроводных клиентов Этого раздела VLAN этого документа с этими параметрами конфигурации:Название ПУЛА DHCP: VLAN 4Сеть ПУЛА DHCP: 10.4.0.0Маска подсети: 255.255.0.0Стартовый IP: 10.4.1.5Конечный IP: 10.4.1.10Маршрутизатор по умолчанию: 10.4.1.1

Настройте аутентификацию WPA

WPA на основе стандартов, совместимое улучшение безопасности, которое строго увеличивает уровень защиты данных и управления доступом для существующих и будущих систем беспроводной локальной сети. Управление ключами WPA поддерживает два взаимоисключающих типа управления: WPA и WPA-PSK.

См. Использование управления ключами WPA для получения дополнительной информации.

Использование управления ключами WPA, клиентов и сервера проверки подлинности аутентифицируется друг на друге использующем метод аутентификации EAP, и клиент и сервер генерирует попарный главный ключ (PMK). Использование WPA, сервер генерирует PMK динамично и передает его к AP.

Данный пример использует эти параметры конфигурации для аутентификации WPA:

- Название SSID: **wpa**
- Идентификатор VLAN: **5**
- IP-адрес VLAN: **10.5.1.1/16**
- Диапазон адресов DHCP для беспроводных клиентов этой VLAN/SSID: **10.5.1.5/16 - 10.5.1.10/16**

Выполните эти шаги для настройки аутентификации WPA:

1. Повторите, что шаги 1 и 2 Настраивают Открытый с Проверкой подлинности MAC, чтобы создать и настроить VLAN с этими параметрами конфигурации:Идентификатор VLAN: 5IP-адрес радиоинтерфейса: 10.5.1.1маска подсети: 255.255.0.0
2. Поскольку WPA является стандартом управления ключами, настройте шифр, который будет использоваться для управления ключами WPA.На беспроводной домашней странице выберите **Wireless Security> Encryption Manager** для настройки настроек шифрования.На экране Wireless Security> Encryption Manager на Безопасности: страница Encryption Manager, войдите **5** для Режима шифрования Набора и Ключей для VLAN.Выберите **Cipher** в качестве Режима шифрования и выберите алгоритм шифрования Cipher из раскрывающегося окна.Данный пример использует **TKIP** в качестве алгоритма Шифра:**Примечание:** В то время как настройка несколько серверов проверок подлинности вводит на беспроводном маршрутизаторе через SDM, иногда не могло бы быть возможно настроить два других типа проверки подлинности оба режима шифрования шифра использования на том же маршрутизатор. В таких случаях настройка шифрования, настроенная через SDM, не могла бы быть применена на маршрутизатор. Для преодоления этого настройте те типы проверки подлинности через CLI.
3. Следующий шаг должен настроить локальный сервер RADIUS для аутентификации клиента. Для выполнения этого повторите, что шаги 3a к 3c Настраивают Открытый с Проверкой подлинности MAC с этими параметрами конфигурации:IP-адрес сервера RADIUS: 10.5.1.1Общий secret: ciscoПрокрутите страницу **Server Manager вниз** для поиска раздела Приоритетов Сервера По умолчанию. В этом разделе выберите этот сервер RADIUS **(10.5.1.1)** в качестве сервера приоритета по умолчанию для Аутентификации eap как показано в данном примере:Повторите, что шаги 3e и 3f Настраивают Открытый с Проверкой подлинности MAC.Повторите, что шаги 3g и 3 h Настраивают Открытый с Проверкой подлинности MAC с этими параметрами конфигурации для Аутентификации eap:IP-адрес клиента AAA: 10.5.1.1Общий secret: ciscoПод разделом Отдельных пользователей настройте имя пользователя и пароль как **user2**.
4. Для включения WPA для SSID необходимо включить Открытый с EAP или Сетевым EAP на SSID. Чтобы к EAP Сети enable, на домашней странице Приложения беспроводной связи, выбирают **Wireless Security> SSID Manager** для настройки SSID и типа проверки подлинности.На Безопасности: страница SSID Manager, настройте SSID и назначьте SSID на VLAN, созданную в step1 для включения SSID на радиоинтерфейсе.Под разделом параметров аутентификации этой страницы выберите **Open Authentication** и из соответствующего раскрывающегося окна, выберите **EAP Authentication**. Кроме того, выберите **Сетевой** тип **Аутентификации eap**.Для настройки Приоритетов Сервера выберите**, Customize** под EAP Аутентифицируют Серверы и выбирают IP-адрес локального сервера RADIUS **10.5.1.1**.Вот пример, который объясняет эти шаги:
5. Прокрутите страницу SSID Manager вниз для поиска **Аутентифицируемого** раздела

Управления ключами.

6. В этом разделе выберите **Mandatory** из раскрывающегося окна Управления ключами и включите **флажок WPA**.Вот окно конфигурации, которое объясняет эти шаги:
7. **Щелкните "Применить".**
8. Для настройки внутреннего сервера DHCP для беспроводных клиентов этой VLAN выполните те же шаги, объясненные в, Настраивают Внутренний сервер DHCP для Беспроводных клиентов Этого раздела VLAN этого документа с этими параметрами конфигурации:Название ПУЛА DHCP: VLAN 5Сеть ПУЛА DHCP: 10.5.0.0Маска подсети: 255.255.0.0Стартовый IP: 10.5.1.5Конечный IP: 10.5.1.10Маршрутизатор по умолчанию: 10.5.1.1

Настройте аутентификацию WPA-PSK

Другой тип управления ключами WPA называют WPA-PSK. WPA-PSK Используется для поддержки WPA на беспроводной локальной сети, где основанная на 802.1x аутентификация не доступна. С этим типом необходимо настроить предварительный общий ключ на AP. Можно ввести предварительный общий ключ как ASCII или шестнадцатеричные символы. При вводе ключа как ASCII - символов вы входите между 8 и 63 символами, и AP разворачивает ключ с помощью процесса, описанного в Основанном на пароле Стандарте Криптографии (RFC2898). При вводе ключа как шестнадцатеричных символов необходимо ввести 64 шестнадцатеричных символа.

Данный пример использует эти параметры конфигурации для аутентификации WPA-PSK:

- Название SSID: **wpa-psk**
- Идентификатор VLAN: **6**
- IP-адрес VLAN: **10.6.1.1/16**
- Диапазон адресов HCP для беспроводных клиентов этой VLAN/SSID: **10.6.1.5/16 - 10.6.1.10/16**

Выполните эти шаги для настройки WPA-PSK:

1. Повторите, что шаги 1 и 2 Настраивают Открытый с Проверкой подлинности MAC, чтобы создать и настроить VLAN с этими параметрами конфигурации:Идентификатор VLAN: 6IP-адрес радиоинтерфейса: 10.6.1.1маска подсети: 255.255.0.0
2. Поскольку WPA-PSK является стандартом управления ключами, настройте шифр, который будет использоваться для управления ключами WPA.На беспроводной домашней странице выберите **Wireless Security> Encryption Manager** для настройки настроек шифрования.На окне **Wireless Security> Encryption Manager** на Безопасности: страница Encryption Manager, войдите **6** для Режима шифрования Набора и Ключей для VLAN.Выберите **Cipher** в качестве Режима шифрования и выберите алгоритм шифрования Cipher из раскрывающегося окна.Данный пример использует **128 битов TKIP+WEP** в качестве алгоритма Шифра.**Примечание:** В то время как настройка несколько серверов проверок подлинности вводит на беспроводном маршрутизаторе через SDM, иногда не могло бы быть возможно настроить два других типа проверки подлинности оба режима шифрования шифра использования на том же маршрутизатор. В таких случаях настройка шифрования, настроенная через SDM, не могла бы быть применена на маршрутизатор. Для преодоления этого настройте те типы проверки подлинности через CLI.
3. Для включения WPA-PSK для SSID необходимо включить открытую аутентификацию

на SSID. Для включения открытой аутентификации повторите, что шаг 6 Настраивает Открытую аутентификацию с Шифрованием WEP.Вот окно конфигурации WPA-PSK:

4. Прокрутите страницу SSID Manager вниз для поиска **Аутентифицируемого** раздела **Управления ключами**.
5. В этом разделе выберите **Mandatory** из раскрывающегося окна Управления ключами, включите **флажок WPA** и введите Предварительный общий ключ WPA в ASCII или Шестнадцатеричный формат.Данный пример использует формат ASCII. Тот же формат должен использоваться в конфигурации клиентской стороны. Вот окно конфигурации, которое объясняет шаг 5:Предварительный общий ключ WPA, используемый в этой конфигурации, 1234567890.
6. **Щелкните "Применить".**
7. Для настройки внутреннего сервера DHCP для беспроводных клиентов этой VLAN выполните те же шаги, объясненные в, Настраивают Внутренний сервер DHCP для Беспроводных клиентов Этого раздела VLAN этого документа с этими параметрами конфигурации:Название ПУЛА DHCP: VLAN 6Сеть ПУЛА DHCP: 10.6.0.0Маска подсети: 255.255.0.0Стартовый IP: 10.6.1.5Конечный IP: 10.6.1.10Маршрутизатор по умолчанию: 10.6.1.1

Конфигурация беспроводного клиента

После настройки ISR через SDM необходимо настроить беспроводного клиента для других типов проверки подлинности так, чтобы маршрутизатор мог аутентифицировать этих беспроводных клиентов и предоставить доступ к сети WLAN. Этот документ использует ADU для конфигурации клиентской стороны.

Настройте беспроводного клиента для открытой аутентификации с шифрованием WEP

Выполните следующие действия:

1. **В окне Profile Management на ADU необходимо нажать New, чтобы создать новый профиль.**Новое окно отображается, где можно установить конфигурацию для открытой аутентификации.
2. **На закладке General ввести имя профиля (Profile Name) и SSID, который будет использоваться клиентским адаптером.**В данном примере Имя профиля и SSID являются **openwep**.**Примечание:** SSID должен совпасть с SSID, который вы настроили на ISR для открытой аутентификации.
3. Нажмите **Вкладку Безопасность** и оставьте параметр безопасности как Предварительный общий ключ (Статический ключ WEP) для Шифрования WEP.
4. Нажмите **Configure** и определите предварительный общий ключ как показано в данном примере:
5. Нажмите **Вкладку Дополнительно** на странице Profile Management и установите Режим аутентификации 802.11 как **Открытый** для открытой аутентификации.
6. Для проверки открытый с аутентификацией WEP, активируйте **openwep** настроенный SSID.
7. Проверьте, что беспроводной клиент привязан успешно с маршрутизатором. Это может быть проверено подробно от беспроводного маршрутизатора с помощью

команды show dot11 associations.Например:`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [openwep] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.1.1.5 CB21AG/PI21AG client self Assoc Others: (not related to any ssid)`

Настройте беспроводного клиента для открытого с проверкой подлинности MAC

Выполните следующие действия:

1. **В окне Profile Management на ADU необходимо нажать New, чтобы создать новый профиль.**Новое окно отображается, где можно установить конфигурацию для открытой аутентификации.
2. **На закладке General ввести имя профиля (Profile Name) и SSID, который будет использоваться клиентским адаптером.**В данном примере Имя профиля и SSID являются **openmac**.**Примечание:** SSID должен совпасть с SSID, который вы настроили на ISR для открытой аутентификации.
3. Нажмите **Вкладку Безопасность** и оставьте параметр безопасности как **Ни один** для открытого с проверкой подлинности MAC. **Затем нажмите кнопку OK.**
4. Для проверки открытый с проверкой подлинности MAC, активируйте **openmac** настроенный SSID.
5. Проверьте, что беспроводной клиент привязан успешно с маршрутизатором. Это может быть проверено подробно от беспроводного маршрутизатора с помощью **команды show dot11 associations**.Например:`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [openmac] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.2.1.5 CB21AG/PI21AG client1 self MAC-Assoc SSID [openwep] : Others: (not related to any ssid)`

Настройте Беспроводного клиента для 802.1X/АУТЕНТИФИКАЦИИ EAP

Выполните следующие действия:

1. **В окне Profile Management на ADU необходимо нажать New, чтобы создать новый профиль.**Новое окно отображается, где можно установить конфигурацию для открытой аутентификации.
2. **На закладке General ввести имя профиля (Profile Name) и SSID, который будет использоваться клиентским адаптером.**В данном примере Имя профиля и SSID являются **скачком**.**Примечание:** SSID должен совпасть с SSID, который вы настроили на ISR для 802.1X/АУТЕНТИФИКАЦИИ EAP.
3. Под менеджментом Профиля нажмите **Вкладку Безопасность**, установите параметр безопасности как **802.1x** и выберите соответствующий тип EAP.Этот документ использует **LEAP** в качестве типа EAP для аутентификации.
4. Нажмите **Configure** для настройки параметров настройки имени пользователя и пароля LEAP.При параметрах настройки имени пользователя и пароля данный пример принимает решение **Вручную Вызвать для Имени пользователя и пароля** так, чтобы клиенту предложили ввести корректное имя пользователя и пароль при попытке соединиться с сетью.
5. **Нажмите кнопку OK.**
6. Для проверки Аутентификации eap активируйте настроенный SSID **скачка**. Вам предлагают ввести имя пользователя и пароль LEAP. Введите обоих учетные данные

как **user1** и нажмите **OK**.

7. Проверьте, что беспроводного клиента аутентифицируют успешно и назначают с IP-адресом. Это может быть проверено ясно от окна состояния ADU.Вот эквивалентные выходные данные от CLI маршрутизатора:`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [leap] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.3.1.5 CB21AG/PI21AG client2 self EAP-Assoc SSID [openmac] : SSID [openwep] : Others: (not related to any ssid)`

Настройте беспроводного клиента для совместно используемой аутентификации

Выполните следующие действия:

1. **В окне Profile Management на ADU необходимо нажать New, чтобы создать новый профиль.**Новое окно отображается, где можно установить конфигурацию для открытой аутентификации.
2. **На закладке General ввести имя профиля (Profile Name) и SSID, который будет использоваться клиентским адаптером.**В данном примере **разделены** Имя профиля и SSID.**Примечание:** SSID должен совпасть с SSID, который вы настроили на ISR для открытой аутентификации.
3. Нажмите **Вкладку Безопасность** и оставьте параметр безопасности как Предварительный общий ключ (Статический ключ WEP) для Шифрования WEP. Затем нажмите **Configure**.
4. Определите предварительный общий ключ как показано в данном примере:
5. **Нажмите кнопку OK.**
6. Под менеджментом Профиля нажмите **Вкладку Дополнительно** и установите Режим аутентификации 802.11 как **Совместно используемый** для совместно используемой аутентификации.
7. Для проверки совместно используемой аутентификации активируйте **совместно используемый** настроенный SSID.
8. Проверьте, что беспроводной клиент привязан успешно с маршрутизатором. Это может быть проверено подробно от беспроводного маршрутизатора с помощью **команды show dot11 associations**.Например:`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [shared] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.4.1.5 CB21AG/PI21AG WCS self Assoc`

Настройте беспроводного клиента для аутентификации WPA

Выполните следующие действия:

1. **В окне Profile Management на ADU необходимо нажать New, чтобы создать новый профиль.**Новое окно отображается, где можно установить конфигурацию для открытой аутентификации.
2. **На закладке General ввести имя профиля (Profile Name) и SSID, который будет использоваться клиентским адаптером.**В данном примере Имя профиля и SSID являются **wpa**.**Примечание:** SSID должен совпасть с SSID, что вы настроили на ISR для WPA (с EAP) аутентификацию.
3. Под менеджментом Профиля нажмите **Вкладку Безопасность**, установите параметр безопасности как **WPA/WPA2/CCKM** и выберите соответствующий тип EAP

WPA/WPA2/CCKM.Этот документ использует **LEAP** в качестве типа EAP для аутентификации.
4. Нажмите **Configure** для настройки параметров настройки имени пользователя и пароля LEAP.При параметрах настройки имени пользователя и пароля данный пример принимает решение **Вручную вызвать для Имени пользователя и пароля** так, чтобы клиенту предложили ввести корректное имя пользователя и пароль при попытке соединиться с сетью.
5. **Нажмите кнопку ОК.**
6. Для проверки Аутентификации eap активируйте настроенный SSID скачка. Вам предлагают ввести имя пользователя и пароль LEAP. Введите обоих учетные данные как **user2**, затем нажмите **OK**.
7. Проверьте, что беспроводного клиента аутентифицируют успешно и назначают с IP-адресом. Это может быть проверено ясно от окна состояния ADU.

Настройте беспроводного клиента для аутентификации WPA-PSK

Выполните следующие действия:

1. **В окне Profile Management на ADU необходимо нажать New, чтобы создать новый профиль.**Новое окно отображается, где можно установить конфигурацию для открытой аутентификации.
2. **На закладке General ввести имя профиля (Profile Name) и SSID, который будет использоваться клиентским адаптером.**В данном примере Имя профиля и SSID являются **wpa-psk**.**Примечание:** SSID должен совпасть с SSID, который вы настроили на ISR для аутентификации WPA-PSK.
3. Под менеджментом Профиля нажмите **Вкладку Безопасность** и установите параметр безопасности как **парольную фразу WPA/WPA2**. Затем нажмите **Configure** для настройки парольной фразы WPA.
4. Определите Предварительный общий ключ WPA. Ключ должен быть 8 - 63 ASCII - символами в длине. **Затем нажмите кнопку ОК.**
5. Для проверки WPA-PSK активируйте настроенный SSID **wpa-psk**.
6. Проверьте, что беспроводной клиент привязан успешно с маршрутизатором. Это может быть проверено подробно от беспроводного маршрутизатора с помощью **команды show dot11 associations**.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Команды для устранения неполадок

Вы можете использовать эти команды debug для устранения неполадок конфигурации.

- **debug dot11 aaa authenticator all — включает процесс отладки аутентификационных пакетов MAC и EAP.**
- **debug radius authentication — отображает связь RADIUS между сервером и клиентом.**
- **debug radius local-server packets — отображает содержание полученных и отправленных**

пакетов RADIUS.
- debug radius local-server client — отображает сообщения об ошибках при неудачных аутентификациях клиентов.

Дополнительные сведения

- Примеры настройки проверки подлинности на контроллерах беспроводной сети
- Настройка VLAN
- Пример настройки беспроводного маршрутизатора 1800 ISR с внутренним DHCP-сервером и открытой аутентификацией
- ISR беспроводной связи Cisco и руководство настройки точки доступа HWIC
- Пример конфигурации подключения к беспроводной локальной сети с использованием маршрутизатора ISR с WEP-шифрованием и LEAP-аутентификацией
- Настройка типов аутентификации
- Пример конфигурации подключения к беспроводной локальной сети с использованием маршрутизатора ISR с WEP-шифрованием и LEAP-аутентификацией
- Cisco Systems – техническая поддержка и документация