Пример настройки типов аутентификации беспроводной связи на фиксированном ISR

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Общие сведения
Настройка
Схема сети
Настройте открытую аутентификацию
Настройте Integrated routing and bridging (IRB) и Установленный Группа мостов
Настройте виртуальный интерфейс моста (BVI)
Настройте SSID для открытой аутентификации
Настройте Внутренний сервер DHCP для Беспроводных клиентов этой VLAN
Настройте 802.1X/АУТЕНТИФИКАЦИЮ EAP
Настройте Integrated routing and bridging (IRB) и Установленный Группа мостов
Настройте виртуальный интерфейс моста (BVI)
Настройте локальный сервер RADIUS для аутентификации eap
Настройте SSID для 802.1X/АУТЕНТИФИКАЦИИ EAP
Настройте Внутренний сервер DHCP для Беспроводных клиентов этой VLAN
Управление ключами WPA
WPA-PSK Настройки
Настройте Integrated routing and bridging (IRB) и Установленный Группа мостов
Настройте виртуальный интерфейс моста (BVI)
Настройте SSID для аутентификации WPA-PSK
Настройте Внутренний сервер DHCP для Беспроводных клиентов этой VLAN
Настройте WPA (с EAP) аутентификация
Настройте Integrated routing and bridging (IRB) и Установленный Группа мостов
Настройте виртуальный интерфейс моста (BVI)
Настройте локальный сервер RADIUS для аутентификации WPA
Настройте SSID для WPA с аутентификацией eap
Настройте Внутренний сервер DHCP для Беспроводных клиентов этой VLAN
Настройте беспроводного клиента для аутентификации
Настройте беспроводного клиента для открытой аутентификации
Настройте Беспроводного клиента для 802.1X/АУТЕНТИФИКАЦИИ EAP
Настройте беспроводного клиента для аутентификации WPA-PSK
Настройте беспроводного клиента для WPA (с EAP) аутентификация

Устранение неполадок
Команды для устранения неполадок
Дополнительные сведения

Введение

Этот документ предоставляет пример конфигурации, который объясняет, как настроить различные типы проверки подлинности Уровня 2 на интегрированном маршрутизаторе фиксированной конфигурации беспроводной связи Cisco для Возможности беспроводного подключения с командами CLI.

Предварительные условия

Требования

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

- Знание того, как настроить основные параметры Cisco ISR (ISR)
- 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
- 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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Маршрутизаторы фиксированной конфигурации интегрированных сервисов Cisco поддерживают безопасное, доступное, и простое в использовании решение для беспроводной локальной сети, которое комбинирует мобильность и гибкость с функциями промышленного класса, требуемыми специалистами по сетевым технологиям. С системой управления на основе программного обеспечения Cisco IOS маршрутизаторы Cisco

действуют как точки доступа и являются сертифицируемым Wi-Fi, IEEE 802.11a/b/g-compliant приемопередатчики беспроводной локальной сети.

Можно настроить и контролировать маршрутизаторы с интерфейсом командной строки (CLI), на основе браузера система управления или Протокол SNMP. Этот документ описывает, как настроить ISR для возможности беспроводного подключения с командами CLI.

Настройка

Данный пример показывает, как настроить эти типы проверки подлинности на беспроводной связи Cisco Интегрированный маршрутизатор фиксированной конфигурации с командами CLI.

- Открытая проверка подлинности
- 802.1x/EAP (Расширяемый протокол аутентификации) аутентификация
- Предварительный общий ключ защищенного доступа по протоколу Wi-Fi (WPA-PSK) аутентификация
- WPA (с EAP) аутентификация

Примечание: Этот документ не фокусируется на совместно используемой аутентификации, так как это - менее защищенный тип проверки подлинности.

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 с аутентификацией 802.1x.

Настройте открытую аутентификацию

Открытая аутентификация является алгоритмом фиктивной проверки подлинности. Точка доступа предоставляет любой запрос об аутентификации. Открытая аутентификация позволяет любой доступ к сети устройства. Если никакое шифрование не включено в сети, никакое устройство, которое знает, SSID точки доступа может получить доступ к сети. С Шифрованием WEP, включенным на точке доступа, сам Ключ WEP становится средством управления доступом. Если устройство не имеет корректного Ключа WEP, даже при том, что аутентификация успешна, устройство неспособно передать данные через точку доступа. И при этом это не может дешифровать данные, передаваемые от точки доступа.

Конфигурация данного примера просто объясняет простую открытую аутентификацию. Ключ WEP может быть сделан обязательным или дополнительным. Данный пример настраивает Ключ WEP как дополнительный так, чтобы любое устройство, которое не использует WEP, могло также аутентифицироваться и связаться с этим AP.

См. Открытую аутентификацию для получения дополнительной информации.

Данный пример использует эту настройку конфигурации для настройки открытой аутентификации на ISR.

- Название SSID: **"открытый"**
- VLAN 1
- Диапазон Внутреннего сервера DHCP: **10.1.0.0/16**

Примечание: Ради простоты данный пример не использует способа шифрования для аутентифицированных клиентов.

Завершите эти действия с маршрутизатором:

1. Настройте Integrated routing and bridging (IRB) и Установленный Группа мостов
2. Настройте виртуальный интерфейс моста (BVI)
3. Настройте SSID для открытой аутентификации
4. Настройте Внутренний сервер DHCP для Беспроводных клиентов этой VLAN

Настройте Integrated routing and bridging (IRB) и Установленный Группа мостов

Завершите эти действия:

1. **Включите IRB в маршрутизаторе.**маршрутизатор <настраивает> **#bridge irbПримечание:** Если все типы безопасности должны быть настроены на одиночном маршрутизаторе, достаточно включить IRB только однажды глобально на маршрутизаторе. Это не должно быть включено для каждого отдельного типа проверки подлинности.
2. **Определите группу мостов.**Данный пример использует номер группы мостов **1**.маршрутизатор <настраивает> *#bridge 1*
3. **Выберите протокол STP для группы мостов.**Здесь, протокол STP IEEE настроен для этой группы мостов.маршрутизатор <настраивает> *протокол IEEE #bridge 1*
4. **Позвольте BVI принять и направить пакеты с возможностью трассировки, полученные от его соответствующей группы мостов.**Данный пример позволяет BVI принять и направить пакет IP.маршрутизатор <настраивает> *ip* **маршрута** *#bridge 1*

Настройте виртуальный интерфейс моста (BVI)

Завершите эти действия:

1. **Настройте BVI.**Настройте BVI при присвоении соответствующего количества группы мостов к BVI. Каждая группа мостов может только иметь один соответствующий интерфейс BVI. Данный пример назначает номер группы моста 1 на BVI.маршрутизатор <настраивает> *#interface BVI <1>*
2. **Присвойте IP-адрес BVI.**маршрутизатор <config-if> **#ip обращается** *10.1.1.1 255.255.0.0*маршрутизатор <config-if> **#no закрывался**

См. Настраивают Мостовое соединение для получения дальнейшей информации на мостовом соединении.

Настройте SSID для открытой аутентификации

Завершите эти действия:

1. **Включите радиоинтерфейс**Для включения радиоинтерфейса перейдите к режиму конфигурации радиоинтерфейса DOT11 и назначьте SSID на интерфейс.маршрутизатор <config> **#interface dot11radio0**маршрутизатор <config-if> **#no завершение**маршрутизатор <config-if> **#ssid** *открытый*Тип открытой аутентификации может быть настроен в сочетании с Аутентификацией с использованием MAC-адреса. В этом случае точка доступа вынуждает все устройства клиента выполнить аутентификацию MAC-address, прежде чем им разрешат присоединиться к сети.Открытая аутентификация может также быть настроена наряду с Аутентификацией eap. Точка доступа вынуждает все устройства клиента выполнить Аутентификацию eap, прежде чем им разрешат присоединиться к сети. Для list-name задайте список способов аутентификации.Точка доступа, настроенная для Аутентификации eap, вызывает все устройства клиента, которые связываются для выполнения Аутентификации eap. Устройства клиента, которые не используют EAP, не могут использовать точку доступа.
2. **Свяжите SSID с VLAN.**Для включения SSID на этом интерфейсе свяжите SSID с VLAN в режиме конфигурации SSID.маршрутизатор *<ssid config> vlan 1*
3. **Настройте SSID с открытой аутентификацией.**маршрутизатор <ssid config> **#authentication открытый**
4. **Настройте радиоинтерфейс для дополнительного Ключа WEP.**маршрутизатор <config> **дополнительный WEP #encryption vlan 1 режима**
5. **Включите VLAN на радиоинтерфейсе.**маршрутизатор <config> **#interface Dot11Radio 0.1**маршрутизатор <config-subif> *#encapsulation dot1Q 1*маршрутизатор <config-subif> *#bridge-group 1*

Настройте Внутренний сервер DHCP для Беспроводных клиентов этой VLAN

Введите эти команды в режиме глобальной конфигурации для настройки внутреннего сервера DHCP для беспроводных клиентов этой VLAN:

- **ip dhcp excluded-address 10.1.1.1 10.1.1.5**
- *ip dhcp pool open*

В режиме настройки пула DHCP введите эти команды:

- *network 10.1.0.0 255.255.0.0*
- **default-router** *10.1.1.1*

Настройте 802.1X/АУТЕНТИФИКАЦИЮ EAP

Этот тип проверки подлинности предоставляет высший уровень безопасности для вашей беспроводной сети. С Протоколом EAP, используемым для взаимодействия с совместимым с EAP сервером RADIUS, точка доступа помогает беспроводному клиентскому устройству и серверу RADIUS выполнять обоюдную проверку подлинности и получать динамический Ключ WEP индивидуальной рассылки. Сервер RADIUS передает Ключ WEP к точке доступа, которая использует его для всех сигналов многоадресных данных, что это передает к или

получает от клиента.

См. Аутентификацию eap для получения дополнительной информации.

Данный пример использует эту настройку конфигурации:

- Название SSID: **скачок**
- VLAN 2
- Диапазон Внутреннего сервера DHCP: **10.2.0.0/16**

Данный пример использует Аутентификацию LEAP в качестве механизма для аутентификации беспроводного клиента.

Примечание: См. Cisco Secure ACS для Windows v3.2 With EAP-TLS Machine Authentication для настройки EAP-TLS.

Примечание: См. Cisco Secure ACS Настройки для Windows v3.2 With PEAP-MS-CHAPv2 Machine Authentication для настройки PEAP-MS-CHAPv2.

Примечание: Поймите, что вся конфигурация этих типов EAP в основном включает изменения конфигурации в клиентской стороне и в стороне сервера проверки подлинности. Конфигурация в беспроводном маршрутизаторе или точке доступа более или менее остается тем же для всех этих типов проверки подлинности.

Примечание: Как упомянуто первоначально, эта настройка использует локальный сервер RADIUS на беспроводном ISR для аутентификации Беспроводных клиентов с аутентификацией 802.1x.

Завершите эти действия с маршрутизатором:

1. Настройте Integrated routing and bridging (IRB) и Установленный Группа мостов
2. Настройте виртуальный интерфейс моста (BVI)
3. Настройте локальный сервер RADIUS для аутентификации eap
4. Настройте SSID для 802.1X/АУТЕНТИФИКАЦИИ EAP
5. Настройте Внутренний сервер DHCP для Беспроводных клиентов этой VLAN

Настройте Integrated routing and bridging (IRB) и Установленный Группа мостов

Завершите эти действия:

1. **Включите IRB в маршрутизаторе.**маршрутизатор <настраивает> **#bridge irbПримечание:** Если все типы безопасности должны быть настроены на одиночном маршрутизаторе, достаточно включить IRB только однажды глобально на маршрутизаторе. Это не должно быть включено для каждого отдельного типа проверки подлинности.
2. **Определите группу мостов.**Данный пример использует номер группы мостов 2.маршрутизатор <настраивает> *#bridge 2*
3. **Выберите протокол STP для группы мостов.**Здесь, протокол STP IEEE настроен для этой группы мостов.маршрутизатор <настраивает> *протокол IEEE #bridge 2*
4. **Выберите протокол STP для группы мостов.**Здесь, протокол STP IEEE настроен для этой группы мостов.маршрутизатор <настраивает> *протокол IEEE #bridge 2*

5. **Позвольте BVI принять и направить пакеты с возможностью трассировки, которые получены от его соответствующей группы мостов.**Данный пример позволяет BVI принять и направить пакеты IP.маршрутизатор <настраивает> *ip* **маршрута** *#bridge 2*

Настройте виртуальный интерфейс моста (BVI)

Завершите эти действия:

1. **Настройте BVI.**Настройте BVI при присвоении соответствующего количества группы мостов к BVI. Каждая группа мостов может только иметь один соответствующий BVI. Данный пример назначает номер группы моста 2 на BVI.маршрутизатор <настраивает> *#interface BVI <2>*
2. **Присвойте IP-адрес BVI.**маршрутизатор <config-if> **#ip обращается** *10.2.1.1 255.255.0.0*маршрутизатор <config-if> **#no закрывался**

Настройте локальный сервер RADIUS для аутентификации eap

Как упомянуто прежде, этот документ использует локальный сервер RADIUS на беспроводном осведомленном маршрутизаторе для Аутентификации eap.

1. **Включите модель управления доступом аутентификации, авторизации и учета (AAA).**маршрутизатор <настраивает> **#aaa новую модель**
2. **Создайте eap рада группы серверов для сервера RADIUS.**маршрутизатор <настраивает> **#aaa сервер** *eap рада* **радиуса сервера группы** *10.2.1.1 acct-порта 1813 подлинного порта 1812*
3. **Создайте список методов eap_methods, который перечисляет метод аутентификации, используемый для аутентификации регистрационной информации пользователя для входа AAA. Назначьте список методов на эту группу серверов.**маршрутизатор <настраивает> **#aaa регистрационное имя для проверки подлинности** *eap_methods eap рада* **группы**
4. **Включите маршрутизатор как локальный сервер проверки подлинности и введите в режим конфигурации для средства проверки подлинности.**маршрутизатор <настраивает> **#radius-server локальную переменную**
5. **В режиме Конфигурации сервера RADIUS добавьте маршрутизатор как клиента AAA локального сервера проверки подлинности.**маршрутизатор <config-radsrv> **#nas** *10.2.1.1* **ключевых** *Cisco*
6. **Настройте пользовательский *user1* на локальном сервере RADIUS.**маршрутизатор <config-radsrv> **#user** *eap рада* **группы** *пароля user1 user1*
7. **Задайте хост сервера RADIUS.**маршрутизатор <config-radsrv> **#radius-server** *Cisco* **ключа** *acct-порта 1813 подлинного порта 1812 хоста 10.2.1.1***Примечание:** Этот ключ должен совпасть с тем, заданным в **nas** команде под режимом конфигурации сервера RADIUS.

Настройте SSID для 802.1X/АУТЕНТИФИКАЦИИ EAP

Конфигурация радиоинтерфейса и связанного SSID для 802.1x/EAP включает конфигурацию различных параметров беспроводной связи на маршрутизаторе, который включает SSID, режим шифрования и тип проверки подлинности. Данный пример

использует SSID, названный *скачком*.

1. **Включите радиоинтерфейс.**Для включения радиоинтерфейса перейдите к режиму конфигурации радиоинтерфейса DOT11 и назначьте SSID на интерфейс.маршрутизатор <config> **#interface dot11radio0**маршрутизатор <config-if> **#no завершение**маршрутизатор <config-if> **#ssid** *скачок*
2. **Свяжите SSID с VLAN.**Для включения SSID на этом интерфейсе свяжите SSID с VLAN в режиме конфигурации SSID.маршрутизатор *<ssid config> #vlan 2*
3. **Настройте SSID с 802.1X/АУТЕНТИФИКАЦИЕЙ LEAP.**маршрутизатор <ssid config> **#authentication сетевой eap** *eap_methods*
4. **Настройте радиоинтерфейс для управления динамического ключа.**маршрутизатор <config> **#encryption шифры режима** *VLAN 2* **wep40**
5. **Включите VLAN на радиоинтерфейсе.**маршрутизатор <config> **#interface Dot11Radio 0.2**маршрутизатор <config-subif> *#encapsulation dot1Q 2*маршрутизатор <config-subif> *#bridge-group 2*

Настройте Внутренний сервер DHCP для Беспроводных клиентов этой VLAN

Введите эти команды в режиме глобальной конфигурации для настройки внутреннего сервера DHCP для беспроводных клиентов этой VLAN:

- **ip dhcp excluded-address 10.2.1.1 10.2.1.5**
- *ip dhcp pool leapauth*

В режиме настройки пула DHCP введите эти команды:

- *network 10.2.0.0 255.255.0.0*
- **default-router** *10.2.1.1*

Управление ключами WPA

Защищенный доступ по протоколу Wi-Fi на основе стандартов, совместимое улучшение безопасности, которое строго увеличивает уровень защиты данных и управления доступом для текущих и будущих систем беспроводной локальной сети.

См. управление ключами WPA для получения дополнительной информации.

Управление ключами WPA поддерживает два взаимоисключающих типа управления: ключ WPA-Pre-Sshared (WPA-PSK) и WPA (с EAP).

WPA-PSK Настройки

WPA-PSK используется в качестве типа управления ключами на беспроводной локальной сети, где основанная на 802.1x аутентификация не доступна. В таких сетях необходимо настроить предварительный общий ключ на точке доступа. Можно ввести предварительный общий ключ как ASCII или шестнадцатеричные символы. При вводе ключа как ASCII - символов вы входите между 8 и 63 символами, и точка доступа разворачивает ключ с процессом, описанным в Основанном на пароле Стандарте Криптографии (RFC2898). При вводе ключа как шестнадцатеричных символов необходимо ввести 64 шестнадцатеричных

символа.

Данный пример использует эту настройку конфигурации:

- Название SSID: **wpa-совместно-используемый**
- VLAN 3
- Диапазон Внутреннего сервера DHCP: **10.3.0.0/16**

Завершите эти действия с маршрутизатором:

1. Настройте Integrated routing and bridging (IRB) и Установленный Группа мостов
2. Настройте виртуальный интерфейс моста (BVI)
3. Настройте SSID для аутентификации WPA-PSK
4. Настройте Внутренний сервер DHCP для Беспроводных клиентов этой VLAN

Настройте Integrated routing and bridging (IRB) и Установленный Группа мостов

Завершите эти действия:

1. **Включите IRB в маршрутизаторе.**маршрутизатор <настраивает> **#bridge irbПримечание:** Если все типы безопасности должны быть настроены на одиночном маршрутизаторе, достаточно включить IRB только однажды глобально на маршрутизаторе. Это не должно быть включено для каждого отдельного типа проверки подлинности.
2. **Определите группу мостов.**Данный пример использует номер группы мостов **3**.маршрутизатор <настраивает> *#bridge 3*
3. **Выберите протокол STP для группы мостов.**Протокол STP IEEE настроен для этой группы мостов.маршрутизатор <настраивает> *протокол IEEE #bridge 3*
4. **Позвольте BVI принять и направить пакеты с возможностью трассировки, полученные от его соответствующей группы мостов.**Данный пример позволяет BVI принять и направить пакеты IP.маршрутизатор <настраивает> *ip* **маршрута** *#bridge 3*

Настройте виртуальный интерфейс моста (BVI)

Завершите эти действия:

1. **Настройте BVI.**Настройте BVI при присвоении соответствующего количества группы мостов к BVI. Каждая группа мостов может только иметь один соответствующий BVI. Данный пример назначает номер группы моста 3 на BVI..маршрутизатор <настраивает> *#interface BVI <2>*
2. **Присвойте IP-адрес BVI.**маршрутизатор <config-if> **#ip обращается** *10.3.1.1 255.255.0.0*маршрутизатор <config-if> **#no закрывался**

Настройте SSID для аутентификации WPA-PSK

Завершите эти действия:

1. **Включите радиоинтерфейс.**Для включения радиоинтерфейса перейдите к режиму конфигурации радиоинтерфейса DOT11 и назначьте SSID на

интерфейс.маршрутизатор <config> **#interface dot11radio0**маршрутизатор <config-if> **#no завершение**маршрутизатор <config-if> **#ssid** *wpa-совместно-используемый*

2. **Для включения управления ключами WPA сначала настройте шифр шифрования WPA для интерфейса виртуальной локальной сети (VLAN). Данный пример использует tkip в качестве шифра шифрования.**.Введите эту команду для определения типа управления ключами WPA на радиоинтерфейсе.маршрутизатор <config> **#interface dot11radio0**маршрутизатор (config-if) **шифры #encryption vlan 3 режима** *tkip*
3. **Свяжите SSID с VLAN.**Для включения SSID на этом интерфейсе свяжите SSID с VLAN в режиме конфигурации SSID.маршрутизатор *<ssid config> vlan 3*
4. **Настройте SSID с аутентификацией WPA-PSK.Необходимо настроить открытую или сетевую Аутентификацию eap сначала в режиме конфигурации SSID для включения управления ключами WPA. Данный пример настраивает открытую аутентификацию.**маршрутизатор <config> **#interface dot11radio0**маршрутизатор <config-if> **#ssid** *wpa-совместно-используемый*маршрутизатор <ssid config> **#authentication открытыйТеперь, включите управление ключами WPA на SSID. Шифр управления ключами tkip уже настроен для этой VLAN.**маршрутизатор (ssid config-if) **#authentication управление ключами wpaНастройте аутентификацию WPA-PSK на SSID.**маршрутизатор *(ssid config-if) #wpa-psk ascii 1234567890****!---1234567890 является значением предварительного общего ключа для этого SSID. Гарантируйте, что тот же ключ задан для этого SSID в клиентской стороне.***
5. **Включите VLAN на радиоинтерфейсе.**маршрутизатор <config> **#interface Dot11Radio 0.3**маршрутизатор <config-subif> *#encapsulation dot1Q 3*маршрутизатор <config-subif> *#bridge-group 3*

Настройте Внутренний сервер DHCP для Беспроводных клиентов этой VLAN

Введите эти команды в режиме глобальной конфигурации для настройки внутреннего сервера DHCP для беспроводных клиентов этой VLAN:

- **ip dhcp excluded-address 10.3.1.1 10.3.1.5**
- *ip dhcp pool wpa-psk*

В режиме настройки пула DHCP введите эти команды:

- *network 10.3.0.0 255.255.0.0*
- **default-router** *10.3.1.1*

Настройте WPA (с EAP) аутентификация

Это - другой тип управления ключами WPA. Здесь, клиенты и сервер проверки подлинности аутентифицируются друг на друге с методом аутентификации EAP, и клиент и сервер генерирует попарный главный ключ (PMK). С WPA сервер генерирует PMK динамично и передает его к точке доступа, но с WPA-PSK вы настраиваете предварительный общий ключ и на клиенте и на точке доступа, и тот предварительный общий ключ используется в качестве PMK.

См. WPA с Аутентификацией eap для получения дополнительной информации.

Данный пример использует эту настройку конфигурации:

- Название SSID: **wpa-dot1x**
- VLAN 4
- Диапазон Внутреннего сервера DHCP: **10.4.0.0/16**

Завершите эти действия с маршрутизатором:

1. Настройте Integrated routing and bridging (IRB) и Установленный Группа мостов
2. Настройте виртуальный интерфейс моста (BVI)
3. Настройте локальный сервер RADIUS для аутентификации WPA.
4. Настройте SSID для WPA с аутентификацией eap
5. Настройте Внутренний сервер DHCP для Беспроводных клиентов этой VLAN

Настройте Integrated routing and bridging (IRB) и Установленный Группа мостов

Завершите эти действия:

1. **Включите IRB в маршрутизаторе.**маршрутизатор <настраивает> **#bridge irbПримечание:** Если все типы безопасности должны быть настроены на одиночном маршрутизаторе, достаточно включить IRB только однажды глобально на маршрутизаторе. Это не должно быть включено для каждого отдельного типа проверки подлинности.
2. **Определите Группу мостов.**Данный пример использует номер группы мостов **4**.маршрутизатор <настраивает> *#bridge 4*
3. **Выберите протокол STP для группы мостов.**Здесь, протокол STP IEEE настроен для этой группы мостов.маршрутизатор <настраивает> *протокол IEEE #bridge 4*
4. **Позвольте BVI принять и направить пакеты с возможностью трассировки, полученные от его соответствующей группы мостов.**Данный пример позволяет BVI принять и направить пакеты IP.маршрутизатор <настраивает> *ip* **маршрута** *#bridge 4*

Настройте виртуальный интерфейс моста (BVI)

Завершите эти действия:

1. **Настройте BVI.**Настройте BVI при присвоении соответствующего количества группы мостов к BVI. Каждая группа мостов может только иметь один соответствующий интерфейс BVI. Данный пример назначает номер группы моста 4 на BVI.маршрутизатор <настраивает> *#interface BVI <4>*
2. **Присвойте IP-адрес BVI.**маршрутизатор <config-if> **#ip обращается** *10.4.1.1 255.255.0.0*маршрутизатор <config-if> **#no закрывался**

Настройте локальный сервер RADIUS для аутентификации WPA

См. раздел под 802.1X/АУТЕНТИФИКАЦИЕЙ EAP для подробной процедуры.

Настройте SSID для WPA с аутентификацией eap

Завершите эти действия:

1. **Включите Радиоинтерфейс.**Для включения радиоинтерфейса перейдите к режиму

конфигурации радиоинтерфейса DOT11 и назначьте SSID на интерфейс.маршрутизатор <config> **#interface dot11radio0**маршрутизатор <config-if> **#no завершение**маршрутизатор <config-if> **#ssid** *wpa-dot1x*
2. **Для включения управления ключами WPA сначала настройте шифр шифрования WPA для интерфейса виртуальной локальной сети (VLAN). Данный пример использует tkip в качестве шифра шифрования..**Введите эту команду для определения типа управления ключами WPA на радиоинтерфейсе.маршрутизатор <config> **#interface dot11radio0**маршрутизатор (config-if) **шифры #encryption vlan 4 режима** *tkip*
3. **Свяжите SSID с VLAN.**Для включения SSID на этом интерфейсе свяжите SSID с VLAN в режиме конфигурации SSID.*vlan 4*
4. **Настройте SSID с аутентификацией WPA-PSK.**Для настройки радиоинтерфейса для WPA с Аутентификацией eap сначала настройте связанный SSID для сети EAP.маршрутизатор <config> **#interface dot11radio0**маршрутизатор <config-if> **#ssid** *wpa-совместно-используемый*маршрутизатор <ssid config> **#authentication сеть eap** *eap_methods*
5. **Теперь, включите управление ключами WPA на SSID. Шифр управления ключами tkip уже настроен для этой VLAN.**маршрутизатор (ssid config-if) **#authentication управление ключами wpa**
6. **Включите VLAN на радиоинтерфейсе.**маршрутизатор <config> **#interface Dot11Radio 0.4**маршрутизатор <config-subif> *#encapsulation dot1Q 4*маршрутизатор <config-subif> *#bridge-group 4*

Настройте Внутренний сервер DHCP для Беспроводных клиентов этой VLAN

Введите эти команды в режиме глобальной конфигурации для настройки внутреннего сервера DHCP для беспроводных клиентов этой VLAN:

- **ip dhcp excluded-address 10.4.1.1 10.4.1.5**
- *ip dhcp pool wpa-dot1shared*

В режиме настройки пула DHCP введите эти команды:

- *network 10.4.0.0 255.255.0.0*
- **default-router** *10.4.1.1*

Настройте беспроводного клиента для аутентификации

После того, как вы настроите ISR, настроите беспроводного клиента для других типов проверки подлинности, как объяснено так, чтобы маршрутизатор мог аутентифицировать этих беспроводных клиентов и предоставить доступ к сети WLAN. Этот документ использует утилиту Cisco Aironet Desktop Utility (ADU) для клиентской конфигурации.

Настройте беспроводного клиента для открытой 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. Под **Вкладкой Общие** введите Имя профиля и SSID, который

использует клиентский адаптер.В данном примере имя профиля и SSID **открыты**.**Примечание:** SSID должен совпасть с SSID, который вы настроили на ISR для открытой аутентификации.
2. Нажмите **Вкладку Безопасность** и оставьте параметр безопасности как **Ни один** для Шифрования WEP. Так как данный пример использует WEP, поскольку дополнительный, устанавливая эту опцию ни в Один позволит клиенту успешно связываться и связываться с сетью WLAN.**Нажмите кнопку ОК**
3. Выберите **окно Advanced** от вкладки **Profile Management** и установите Режим аутентификации 802.11 как **Открытый** для открытой аутентификации.

Этот раздел позволяет убедиться, что конфигурация работает правильно.

1. После того, как клиентский профиль создан, нажмите **Activate** под вкладкой Profile Management для активации профиля.
2. Проверьте статус ADU для успешной аутентификации.

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. Под **Вкладкой Общие** введите Имя профиля и SSID, который использует клиентский адаптер.В данном примере имя профиля и SSID являются **скачком**.
2. 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. Теперь, нажмите **Configure** для настройки параметров настройки имени пользователя и пароля LEAP.**Примечание:** Примечание: SSID должен совпасть с SSID, который вы настроили на ISR для 802.1X/АУТЕНТИФИКАЦИИ EAP.
3. 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, в то время как клиент пытается соединиться с сетью. **Нажмите кнопку ОК.**

Этот раздел позволяет убедиться, что конфигурация работает правильно.

- После того, как клиентский профиль создан, нажмите **Activate** под вкладкой **Profile Management** для активации **скачка** профиля. Вам предлагают для имени и пароля **пользователя LEAP**. Данный пример использует **имя пользователя и пароль user1**. **Нажмите кнопку ОК.**
- Можно наблюдать, что клиент аутентифицируется успешно и назначен IP-адрес от сервера DHCP, настроенного на маршрутизаторе.

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. Под **Вкладкой Общие** введите **Имя профиля** и **SSID**, который использует клиентский адаптер.В данном примере **wpa-разделены** имя профиля и SSID.**Примечание:** SSID должен совпасть с SSID, который вы настроили на ISR для аутентификации WPA-PSK.

2. Под **менеджментом Профиля** нажмите **Вкладку Безопасность** и установите параметр безопасности как **парольную фразу WPA/WPA2**. Теперь, нажмите **Configure** для настройки парольной фразы WPA.
3. Определите Предварительный общий ключ WPA. Ключ должен быть 8 - 63 ASCII - символами в длине. **Нажмите кнопку ОК.**

Этот раздел позволяет убедиться, что конфигурация работает правильно.

- После того, как клиентский профиль создан, нажмите **Activate** под вкладкой **Profile Management** для активации **wpa-разделенного** профиля.
- Проверьте ADU для успешной аутентификации.

Настройте беспроводного клиента для WPA (с EAP) аутентификация

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. Под **Вкладкой Общие** введите Имя профиля и SSID, который использует клиентский адаптер.В данном примере имя профиля и SSID являются **wpa-dot1x**.**Примечание:** SSID должен совпасть с SSID, что вы настроили на ISR для WPA (с EAP) аутентификацию.
2. Под **менеджментом Профиля** нажмите **Вкладку Безопасность**, установите параметр безопасности как **WPA/WPA2/CCKM**, и и выберите соответствующий тип EAP WPA/WPA2/CCKM. Этот документ использует LEAP в качестве типа EAP для аутентификации. Теперь, нажмите **Configure** для настройки параметров настройки имени пользователя и пароля LEAP.
3. Под областью Username and Password Settings данный пример принимает решение **Вручную Вызвать для Имени пользователя и пароля** так, чтобы клиенту предложили ввести корректное имя пользователя и пароль, в то время как клиент пытается соединиться с сетью. **Нажмите кнопку ОК.**

Этот раздел позволяет убедиться, что конфигурация работает правильно.

1. После того, как клиентский профиль создан, нажмите **Activate** под вкладкой Profile Management для активации **wpa-dot1x** профиля. Вам предлагают для имени и пароля Пользователя LEAP. Данный пример использует имя пользователя и пароль в качестве **user1**. **Нажмите кнопку ОК.**
2. Можно наблюдать, что клиент аутентифицируется успешно.

Команда show dot11 associations от CLI маршрутизатора отображает полное изложение на статусе связывания клиента. Например.

Ассоциации dot11 Router#show

```
802.11 Client Stations on Dot11Radio0:
```

```
SSID [leap] :

MAC Address IP address Device Name Parent State 0040.96ac.e657 10.3.0.2 CB21AG/PI21AG WCS self
EAP-Assoc SSID [open] : SSID [pre-shared] : DISABLED, not associated with a configured VLAN SSID
[wpa-dot1x] : SSID [wpa-shared] : Others: (not related to any ssid)
```

Устранение неполадок

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
- VLAN Настройки на точках доступа
- 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
- Cisco Systems – техническая поддержка и документация
- Настройка типов аутентификации
- Пример конфигурации подключения к беспроводной локальной сети с использованием маршрутизатора ISR с WEP-шифрованием и LEAP-аутентификацией