PEAP под Unified Wireless Networks с Microsoft Internet Authentication Service (IAS)

Содержание

Введение

В этом документе приведен пример настройки защищенного расширяемого протокола аутентификации (PEAP) с протоколом аутентификации версии 2 в унифицированной беспроводной сети Cisco (UWN) со службой интернет-аутентификации Microsoft (IAS) в качестве сервера RADIUS.

Предварительные условия

Требования

Существует предположение, что читатель ознакамливается с основной установкой Windows 2003 и установкой контроллера Cisco, так как этот документ только покрывает определенные конфигурации для упрощения тестов.

Примечание: Этот документ предназначен, чтобы дать читателям пример на конфигурации, требуемой на сервере MS для PEAP – Аутентификация CHAP MS. Конфигурация сервера Microsoft, представленная в этом разделе, была протестирована в лабораторной работе и, как находили, работала как ожидалось. При наличии затруднений при настройке сервера Microsoft свяжитесь с Microsoft для справки. Центр технической поддержки Cisco не поддерживает конфигурацию Microsoft Windows server.

Для начальной установки и сведений о конфигурации для Cisco Контроллеры серии 4400, обратитесь к Краткому руководству по началу работы: Контроллеры беспроводных LAN серии Cisco 4400.

Установка Microsoft Windows 2003 года и руководства по конфигурации могут быть найдены при Установке Windows Server 2003 R2.

Перед началом установите Microsoft Windows server 2003 с операционной системой SP1 на каждом из серверов в тестовой лабораторной работе и обновите все Пакеты обновления. Установите контроллеры и облегченные точки доступа (LAP) и гарантируйте, что настроены обновления последних версий программного обеспечения.

Используемые компоненты

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

- Контроллер Cisco серии 4400, который выполняет версию микропрограммы 4.0
- AP протокола LWAPP Cisco 1131
- Windows 2003 Enterprise server (SP1) с Интернет-сервисом проверки подлинности (IAS), Центром сертификации (CA), DHCP и сервисами Системы доменных имен (DNS) установлен
- Windows XP Professional с SP 2 (и обновленные Пакеты обновления) и Cisco Aironet 802.11a/b/g адаптер беспроводной связи (NIC)
- Версия 4.0 служебной программы рабочего стола Aironet
- Коммутатор Cisco 3560

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.

Обзор PEAP

PEAP использует безопасность транспортного уровня (TLS) для создания зашифрованного канала между аутентифицирующимся клиентом PEAP, таким как беспроводной портативный ПК, и средством проверки подлинности PEAP, таким как Microsoft Internet Authentication Service (IAS) или любой сервер RADIUS. PEAP не задает метод аутентификации, но предоставляет дополнительные меры безопасности для других протоколов Аутентификации eap, таких как EAP-MSCHAPv2, который может работать через зашифрованный канал TLS, предоставленный PEAP. Процесс аутентификации PEAP состоит из двух основных этапов:

Фаза 1 PEAP: TLS зашифровал канал

Беспроводной клиент связывается с AP. Основанная на IEEE 802.11 ассоциация предоставляет Открытую систему или Проверку подлинности с общим ключом, прежде чем безопасная ассоциация будет создана между клиентом и точкой доступа (LAP). После того, как основанная на IEEE 802.11 ассоциация успешно установлена между клиентом и точкой доступа, о сеансе TLS выполняют согласование с AP. После того, как аутентификация успешно завершена между Беспроводным клиентом и сервером IAS, о сеансе TLS выполняют согласование между ними. Ключ, который получен в этом согласовании, используется для шифрования всей последующей связи.

Фаза PEAP два: аутентифицируемая на EAP связь

Связь EAP, которая включает согласование EAP, происходит в канале TLS, созданном PEAP в первом этапе процесса аутентификации PEAP. Сервер IAS аутентифицирует Беспроводного клиента с MS-CHAP EAP v2. LAP и Контроллер только передают сообщения между Беспроводным клиентом и сервером RADIUS. WLC и LAP не могут дешифровать эти сообщения, потому что это не оконечная точка TLS.

После того, как этап один PEAP происходит, и канал TLS создан между сервером IAS и Беспроводным клиентом 802.1X для попытки успешной аутентификации, где пользователь предоставил основанные на правильном пароле учетные данные PEAP-MS-CHAP v2, последовательность Сообщения RADIUS - это:

1. Сервер IAS передает идентификационное сообщение запроса клиенту: EAP-Request/Identity.
2. Клиент отвечает идентификационным ответным сообщением: EAP-Response/Identity.
3. Сервер IAS передает Challenge - сообщение MS-CHAP v2: EAP-Request/EAP-Type=EAP MSCHAPV2 (проблема).
4. Клиент отвечает проблемой MS-CHAP v2 и ответом: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Ответ).
5. Когда сервер успешно аутентифицировал клиента, сервер IAS передает пакет MS-CHAP v2 успеха обратно: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Успех).
6. Когда клиент успешно аутентифицировал сервер, клиент отвечает пакетом MS-CHAP v2 успеха: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Успех).
7. Сервер IAS передает TLV EAP, который указывает на успешную аутентификацию.
8. Клиент отвечает сообщением об успешном завершении статуса TLV EAP.
9. Сервер завершает аутентификацию и передает Сообщение об успешном завершении EAP с помощью простого текста. Если VLAN развернуты для клиентской изоляции, атрибуты VLAN включены в это сообщение.

Настройка

Этот документ предоставляет пример для конфигурации PEAP MS-CHAP v2.

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:

В этой настройке Microsoft Windows 2003 Server выполняет эти роли:

- Контроллер домена для доменного **Wireless.com**
- DHCP/СЕРВЕР DNS
- Сервер Центра сертификации (CA)
- Active Directory – для поддержания базы данных пользователей
- Интернет-сервис проверки подлинности (IAS) – для аутентификации Пользователей беспроводной связи

Этот сервер соединяется с проводной сетью через Коммутатор уровня 2 как показано.

Контроллер беспроводной локальной сети (WLC) и зарегистрированный LAP также соединяются с сетью через Коммутатор уровня 2.

Беспроводные клиенты C1 и C2 будут использовать Защищенный доступ по протоколу Wi-Fi 2 (WPA2) - аутентификация PEAP MSCHAP v2 для соединения с Беспроводной сетью.

Цель состоит в том, чтобы настроить сервер Microsoft 2003, Контроллер беспроводной локальной сети и AP Легкого веса для аутентификации Беспроводных клиентов с аутентификацией PEAP MSCHAP v2.

Следующий раздел объясняет, как настроить устройства для этой настройки.

Конфигурации

Этот раздел посмотрел на конфигурацию, требуемую устанавливать Аутентификацию PEAP MS-CHAP v2 в этом WLAN:

- Настройте Microsoft Windows 2003 Server
- Настройте контроллер беспроводной локальной сети (WLC) и AP легкого веса
- Настройте беспроводных клиентов

Запустите с конфигурации Microsoft Windows 2003 Server.

Настройте Microsoft Windows 2003 Server

Настройте Microsoft Windows 2003 Server

Как упомянуто в разделе Сетевой установки, используйте Microsoft Windows 2003 Server в сети для выполнения этих функций.

- **Контроллер домена** – для доменных **беспроводных сетей**
- **DHCP/СЕРВЕР DNS**
- **Сервер Центра сертификации (CA)**
- **Интернет-сервис проверки подлинности (IAS)** – для аутентификации Пользователей беспроводной связи
- **Active Directory** – для поддержания базы данных пользователей

Настройте Microsoft Windows 2003 Server для этих сервисов. Начните с конфигурации Microsoft Windows 2003 Server как Контроллер домена.

Настройте Microsoft Windows 2003 Server как Контроллер домена

Для настройки Microsoft Windows 2003 Server как Контроллера домена выполните эти шаги:

1. Нажмите **Start**, нажмите **Run**, введите **dcpromo.exe**, и затем нажмите **OK** для начала Мастера Установки Active Directory.
2. Нажмите **Next** для выполнения Мастера Установки Active Directory.
3. Для создания нового домена выберите **опцию Domain Controller** для нового домена.
4. Нажмите **Next** для создания нового леса деревьев домена.
5. Если DNS не установлен в системе, мастер предоставляет вас опции, с которыми можно настроить DNS. Выберите **No, Just Install и Configure DNS** на этом компьютере. **Нажмите кнопку Next.**
6. Введите полное имя DNS для нового домена. В данном примере используется **Wireless.com**, и нажмите **Next**.
7. Введите ИМЯ NETBIOS для домена и нажмите **Next**. Данный пример использует **БЕСПРОВОДНЫЕ СЕТИ**.
8. Выберите базу данных и регистрируйте местоположения для домена. **Нажмите кнопку Next.**
9. Выберите местоположение для папки Sysvol. **Нажмите кнопку Next.**
10. Выберите разрешения по умолчанию для пользователей и групп. **Нажмите кнопку Next.**
11. Установите Пароль администратора и нажмите **Next**.
12. Нажмите **Next** для принятия набора Параметров домена ранее.
13. Нажмите **Finish** для закрытия Мастера Установки Active Directory.
14. Перезапустите сервер для изменений для вступления в силу.

С этим шагом вы настроили Microsoft Windows 2003 Server как Контроллер домена и создали новый доменный **Wireless.com**. Затем настройте сервисы DHCP на сервере.

Установите и настройте сервисы DHCP на Microsoft Windows 2003 Server

Сервис DHCP на сервере Microsoft 2003 используется для обеспечения IP-адресов Беспроводным клиентам. Чтобы установить и настроить сервисы DHCP на этом сервере, выполните эти шаги:

1. **Нажмите Add или удалите программы** в панели управления.
2. Нажмите **Add/Remove Windows Components**.
3. Выберите **Networking Services** и нажмите **Details**.
4. Выберите **Dynamic Host Configuration Protocol (DHCP)** и нажмите **OK**.
5. Нажмите **Next** для установки сервиса DHCP.

6. **Для завершения установки нажмите кнопку Finish.**
7. Для настройки сервисов DHCP нажмите **Пуск> Программы> Средства администрирования** и нажмите моментальный снимок **DHCP** - в.
8. Выберите сервер DHCP - **tsweb-lapt.wireless.com** (в данном примере).
9. Нажмите **Action** и затем нажмите **Authorize** для авторизации сервиса DHCP.
10. В Дереве консоли щелкните правой кнопкой мыши **tsweb-lapt.wireless.com** и затем нажмите **New Scope** для определения Диапазона IP-адресов для Беспроводных клиентов.
11. На Приветствии к странице New Scope Wizard Нового Мастера создания области нажмите **Next**.
12. На странице Scope Name введите имя области DHCP. В данном примере используйте **Клиентов DHCP** в качестве названия области. **Нажмите кнопку Next.**
13. На странице IP Address Range введите запуск и закончите IP-адреса для области и нажмите **Next**.
14. На странице Add Exclusions упомяните IP-адрес, который требуется резервировать/исключить от области DHCP. **Нажмите кнопку Next.**
15. Упомяните продолжительность аренды на странице Lease Duration и нажмите **Next**.
16. На Настраивать странице параметров DHCP выберите **Yes, I want to configure DHCP Option now** и нажмите **Next**.
17. Если существует маршрутизатор основного шлюза, упомяните IP-адрес маршрутизатор/шлюза на странице (Default Gateway) маршрутизатора и нажмите **Next**.
18. На Доменном имени и странице серверов DNS, введите имя домена, который был настроен ранее. В примере используйте **Wireless.com**. Введите IP-адрес сервера. **Нажмите Add.**
19. **Нажмите кнопку Next.**
20. На Странице сервера WINS нажмите **Next**.
21. На Активировать странице Scope выберите **Yes, I want to activate the scope now** и нажмите **Next**.
22. При завершении Нового Мастера создания области нажмите **Finish**.
23. В окне DHCP Snapin проверьте, что область DHCP, которая была создана, активна.

Теперь, когда DHCP / DNS включен на сервере, настройте сервер как предприятие сервер Центра сертификации (CA).

Установите и настройте Microsoft Windows 2003 Server как сервер центра сертификации (CA)

PEAP с EAP-MS-CHAPv2 проверяет сервер RADIUS на основе подарка сертификата на сервере. Кроме того, серверный сертификат должен быть выполнен общим центром сертификации (CA), которому доверяет компьютер клиента (т.е. общий сертификат CA уже существует в папке Trusted Root Certification Authority на хранилище сертификата компьютера клиента). В данном примере настройте Microsoft Windows 2003 Server как Центр сертификации (CA), который выполняет сертификат к Интернет-сервису проверки подлинности (IAS).

Чтобы установить и настроить сервисы сертификации на сервере, выполните эти шаги:

1. **Нажмите Add или Удалите программы в Панели управления**.

2. Нажмите **Add/Remove Windows components**.
3. Нажмите **Certificate Services**.
4. Нажмите **Yes** к предупреждающему сообщению **После Установки Сервисов сертификации, компьютер не может быть переименован, и компьютер не может присоединиться или быть удален из домена. Вы хотите продолжить?**
5. Под Типом Центра сертификации выберите **узел CA Enterprise** и нажмите **Next**.
6. Введите имя для определения **БЕСПРОВОДНОГО CA.** использования Данного примера CA. **Нажмите кнопку Next.**
7. Каталог “Cert Log” создан для хранилища базы данных сертификата. **Нажмите кнопку Next.**
8. Если IIS включен, это должно быть, остановился перед переходом. Нажмите **OK** к предупреждающему сообщению, что должен быть остановлен IIS. Это перезапускает автоматически, после CA установлен.
9. Нажмите **Finish** для завершения установки сервисов Центра сертификации (CA).

Следующий шаг должен установить и настроить интернет-Сервис проверки подлинности на Microsoft Windows 2003 Server.

Подключите клиентов с доменом

Следующий шаг должен подключить клиентов с проводной сетью и загрузить зависящую от домена информацию от нового домена. Другими словами, подключите клиентов с доменом. Для этого выполните следующие действия:

1. Подключите клиентов с проводной сетью со сквозным Кабелем Ethernet.
2. Загрузите клиента и войдите с именем пользователя / пароль клиента.
3. **Нажмите кнопку Пуск; нажмите кнопку Run;** введите **cmd**; и нажмите **OK**.
4. В командной строке введите **ipconfig** и нажмите **Enter**, чтобы проверить, что DHCP работает правильно, и клиент получил IP-адрес от сервера DHCP.
5. Для соединения клиента с доменом щелкните правой кнопкой **по My Computer** и выберите **Properties**.
6. **Перейдите на вкладку «Имя компьютера».**
7. **Нажмите кнопку «Изменить».**
8. Нажмите **Domain**; введите **wireless.com**; и нажмите **OK**.
9. Введите **Администратора Имени пользователя** и пароль, определенный для домена, к которому присоединяется клиент. (Это - учетная запись администратора в Active Directory на сервере.)
10. **Нажмите кнопку OK.**
11. Нажмите **Yes** для перезапуска компьютера.
12. Как только компьютер перезапускает, вход в систему с этой информацией: Имя пользователя = **Администратор**; Пароль = **<пароль домена>**; Домен = **беспроводные сети**.
13. Щелкните правой кнопкой **по My Computer** и нажмите **Properties**.
14. Нажмите вкладку **Computer Name**, чтобы проверить, что вы находитесь на домене Wireless.com.
15. Следующий шаг должен проверить, что клиент получил сертификат CA (доверие) от сервера.
16. **Нажмите кнопку Пуск; нажмите кнопку Run;** введите **mmc** и нажмите **OK**.
17. Нажмите **File** и нажмите моментальный снимок **Add/Remove** - в.

18. **Нажмите Add.**
19. Выберите **Certificate** и **нажмите Add**.
20. Выберите **Computer Account** и нажмите **Next**.
21. Нажмите **Finish** для принятия локального компьютера по умолчанию.
22. Нажмите **Close** и нажмите **OK**.
23. Разверните **Сертификаты (Локальный компьютер)**; разверните **Доверенные корневые центры сертификации**; и нажмите **Certificates**. Найдите **беспроводные сети** в списке.
24. Повторите эту процедуру для добавления большего количества клиентов к домену.

Установите интернет-сервис проверки подлинности на Microsoft Windows 2003 Server и запросите сертификат

В этой настройке Интернет-сервис проверки подлинности (IAS) используется в качестве сервера RADIUS для аутентификации Беспроводных клиентов с аутентификацией PEAP.

Выполните эти шаги, чтобы установить и настроить IAS на сервере.

1. **Нажмите Add или удалите программы** в панели управления.
2. Нажмите **Add/Remove Windows Components**.
3. Выберите **Networking Services** и нажмите **Details**.
4. Выберите **Internet Authentication Service**; **нажмите кнопку OK;** и нажмите **Next**.
5. Нажмите **Finish** для завершения установки IAS.
6. Следующий шаг должен установить компьютерный сертификат для Интернет-сервиса проверки подлинности (IAS).
7. **Нажмите кнопку Пуск; нажмите кнопку Run;** введите **mmc**; и нажмите **OK**.
8. Нажмите **Console** в меню Файл, и затем выберите моментальный снимок **Add/Remove** - в.
9. **Нажмите Add** для добавления моментального снимка - в.
10. Выберите **Certificates** из списка моментального-снимка-ins и **нажмите Add**.
11. Выберите **Учетную запись компьютера** и нажмите **Next**.
12. Выберите **Локальный компьютер** и нажмите **Finish**.
13. Нажмите **Close** и нажмите **OK**.
14. Разверните **Сертификаты (Локальный компьютер)**; щелкните правой кнопкой **по Персональной папке**; выберите **All tasks** и затем **Запрос Новый Сертификат**.
15. Нажмите **Next** на ***приветствии мастеру запроса сертификата***.
16. Выберите шаблон сертификата **Контроллера домена** (если вы запрашиваете компьютерный сертификат на сервере кроме DC, выбираете шаблон сертификата **Computer**), и нажмите **Next**.
17. Введите имя и описание для сертификата.
18. Нажмите **Finish** для завершения сертификации запрашивают мастера.

Настройте интернет-Сервис проверки подлинности для Аутентификации PEAP-MS-CHAP v2

Теперь, когда вы установили и запросили сертификат на IAS, настройте IAS для аутентификации.

Выполните следующие действия:

1. Нажмите **Start> Programs> Administrative Tools** и нажмите моментальный снимок **Internet Authentication Service** - в.
2. Щелкните правой кнопкой мыши **Интернет-сервис проверки подлинности (IAS)**, и затем нажмите **Register Service in Active Directory**.
3. Диалоговое окно **Register Internet Authentication Service in Active Directory** появляется; **нажмите кнопку OK.** Это позволяет IAS аутентифицировать пользователей в Active Directory.
4. Нажмите **OK** в следующем диалоговом окне.
5. Добавьте Контроллер беспроводной локальной сети как клиента AAA на сервере IAS MS.
6. Щелкните правой кнопкой мыши **Клиентов RADIUS** и выберите **New RADIUS Client**.
7. Введите имя клиента (WLC в этом случае) и введите IP-адрес WLC. **Нажмите кнопку Next.**
8. На следующей странице, под Клиентом - поставщиком, выбирают **RADIUS Standard**; введите общий секретный ключ; и нажмите **Finish**.
9. Заметьте, что WLC добавлен как клиент AAA на IAS.
10. Создайте политику удаленного доступа для клиентов.
11. Чтобы сделать это, щелкните правой кнопкой мыши **Политику Удаленного доступа** и выберите **New Remote Access Policy**.
12. Введите имя для политики удаленного доступа. В данном примере используйте **PEAP** названия. **Нажмите кнопку Next.**
13. Выберите атрибуты политики на основе своих требований. В данном примере выберите **Wireless**.
14. На следующей странице выберите **User** для применения этой политики удаленного доступа к списку пользователей.
15. Под Методами аутентификации выберите **Protected EAP (PEAP)** и нажмите **Configure**.
16. На странице **Protected EAP Properties** выберите соответствующий сертификат из Сертификата Выполненное раскрывающееся меню и нажмите **OK**.
17. Проверьте подробные данные политики удаленного доступа и нажмите **Finish**.
18. Политика удаленного доступа была добавлена к списку.
19. Щелкните правой кнопкой мыши политику и нажмите **Properties**. Выберите **“Grant remote access permission”** под, “**Если запрос подключения совпадает с указанными условиями**”.

Добавьте пользователей к Active Directory

В этой настройке База данных пользователей поддержана на Active Directory.

Для добавления пользователей к базе данных Active Directory выполните эти шаги:

1. В дереве консоли Пользователей и компьютеров Active Directory щелкните правой кнопкой мыши **Пользователей**; **щелкните New;** и затем нажмите **User**.
2. В Новом Объекте – диалоговое окно User, введите имя Пользователя беспроводной связи. Данный пример использует название **WirelessUser** в поле Имени и **WirelessUser** в Пользовательском поле имени пользователя. **Нажмите кнопку Next.**
3. В Новом Объекте – диалоговое окно User, введите пароль по Вашему выбору в Полях Password и Полях подтверждения пароля. Очиститесь **Пользователь должен изменить пароль в следующем** флажке **входа в систему** и нажать **Next**.

4. В Новом Объекте – диалоговое окно User, нажмите **Finish**.
5. Повторите шаги 2 - 4 для создания дополнительных учетных записей пользователя.

Позвольте беспроводной доступ пользователям

Выполните следующие действия:

1. В дереве консоли **Пользователей и компьютеров Active Directory** нажмите **Папку Пользователи**; щелкните правой кнопкой мыши **WirelessUser**; **нажмите Properties;** и затем перейдите **к Вкладке наборный (телефонный) доступ**.
2. Выберите **предоставляют доступ** и нажимают **OK**.

Настройте контроллер беспроводной локальной сети и легковесные AP

Теперь настройте Беспроводные устройства для этой настройки. Это включает конфигурацию Контроллеров беспроводной локальной сети, Легковесных AP и Беспроводных клиентов.

Настройте WLC для проверки подлинности RADIUS через сервер RADIUS IAS MS

Сначала настройте WLC для использования IAS MS в качестве сервера проверки подлинности. Необходимо настроить WLC для переадресации на внешний сервер RADIUS учетные данные пользователя. Внешний сервер RADIUS проверяет учетные данные пользователя и предоставляет доступ беспроводным клиентам. Чтобы сделать это, добавьте сервер IAS MS как сервер RADIUS на странице **Security> RADIUS Authentication**.

Выполните следующие действия:

1. **Выберите Security и RADIUS Authentication в контроллере GUI, чтобы открыть страницу RADIUS Authentication Servers. Чтобы определить сервер RADIUS, нажмите New.**
2. **Определите параметры сервера RADIUS в RADIUS Authentication Servers > New page.** В их числе: RADIUS Server IP Address, Shared Secret, Port Number и Server Status. С помощью флажков Network User и Management можно определить, применяется ли аутентификация на основе сервера RADIUS для управления и сетевых пользователей. Данный пример использует IAS MS в качестве сервера RADIUS с IP-адресом 10.77.244.198.
3. **Щелкните "Применить".**
4. Сервер IAS MS был добавлен к WLC как сервер RADIUS и может использоваться для аутентификации Беспроводных клиентов.

Настройте WLAN для клиентов

Настройте SSID (WLAN), с которым Беспроводные клиенты соединяется. В данном примере создайте SSID и назовите его **PEAP**.

Определите Аутентификацию Уровня 2 как WPA2 так, чтобы клиенты выполнили, EAP

базировал аутентификацию (MSCHAPv2 PEAP в этом случае), и используйте AES в качестве механизма шифрования. Оставьте все другие значения в их настройках по умолчанию.

Примечание: Этот документ связывает WLAN с интерфейсами управления. Когда у вас есть несколько интерфейсов VLAN в вашей сети, можно создать отдельную VLAN и связать ее с SSID. Для получения информации о том, как настроить VLAN на WLC, обратитесь к VLAN на Примере конфигурации Контроллеров беспроводной локальной сети.

Для настройки WLAN на WLC, выполняют эти шаги:

1. **Выберите WLANs в GUI контроллера, чтобы открыть страницу WLANs.** Эта страница перечисляет WLAN, которые существуют на контроллере.
2. **Чтобы создать новую WLAN, выберите New. Введите идентификатор и SSID для WLAN и нажмите Apply.**
3. **После создания новой WLAN появляется страница WLAN > Edit для новой WLAN.** На этой странице можно определить различные параметры, определенные для этого WLAN, которые включают Общую политику, серверы RADIUS, Политику безопасности и Параметры 802.1x.
4. **Чтобы активировать WLAN, под General Policies проверьте Admin Status. Если необходимо, чтобы AP транслировала SSID в кадрах "неисправность", проверьте Broadcast SSID.**
5. Под безопасностью уровня 2 выберите **WPA1+WPA2**. Это включает WPA на WLAN. Прокрутите страницу вниз и выберите политику WPA. Данный пример использует WPA2 и шифрование AES. В раскрывающемся меню под RADIUS Servers выберите соответствующие серверы RADIUS. В данном примере используйте **10.77.244.198** (IP-адрес сервера IAS MS). Другие параметры могут быть изменены на основе требования сети WLAN.
6. **Щелкните "Применить".**

Настройте беспроводных клиентов

Настройте беспроводных клиентов для MS PEAP аутентификация CHAPv2

Данный пример предоставляет сведения о том, как настроить Беспроводного клиента с утилитой Cisco Aironet Desktop Utility. Прежде чем вы настроите клиентский адаптер, гарантируете, что используется та последняя версия микропрограммного обеспечения и утилиты. Найдите последнюю версию микропрограммного обеспечения и утилит в Странице Wireless downloads на Cisco.com.

Для настройки Беспроводного клиентского адаптера a/b/g 802.11 Cisco Aironet с ADU выполните эти шаги:

1. Откройте служебную программу рабочего стола Aironet.
2. Нажмите **Profile Management** и нажмите **New** для определения профиля.
3. Под Вкладкой Общие введите Имя профиля и SSID. В данном примере используйте SSID, который вы настроили на WLC (PEAP).
4. Выберите Вкладку Безопасность; выберите **WPA/WPA2/CCKM**; под EAP WPA/WPA2/CCKM тип выбирает **PEAP [EAP-MSCHAPv2]** и нажимает **Configure**.

5. Выберите **Validate Server Certificate** и выберите **Wireless-CA** под раскрывающимся меню полномочий Сертификата доверенного корня.
6. **Нажмите OK** и активируйте профиль.**Примечание:** Когда вы используете Защищенную Версию протокола 2 Квитирования с аутентификацией Microsoft EAP (MSCHAPv2 PEAP) с Microsoft XP SP2, и Беспроводной картой управляет Microsoft Wireless Zero Configuration (WZC), необходимо применить заплату Microsoft KB885453. Это предотвращает несколько проблем на аутентификации, отнесенной к PEAP Быстрое Резюме.

Проверка и устранение неполадок

Чтобы проверить, работает ли конфигурация как ожидалось, активируйте MSCHAPv2 PEAP профиля на Client1 Беспроводного клиента.

Как только MSCHAPv2 PEAP профиля активирован на ADU, клиент выполняет открытую аутентификацию 802.11 и затем выполняет аутентификацию MSCHAPv2 PEAP. Вот пример успешной аутентификации MSCHAPv2 PEAP.

Используйте команды отладки для понимания последовательности событий, которые происходят.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Эти команды отладки на Контроллере беспроводной локальной сети полезны.

- **debug dot1x events enable** — Для настройки отладки событий 802.1x
- **debug aaa events enable** — Для настройки отладки событий AAA
- **адрес debug mac <мак адрес>** — Чтобы настроить отладку MAC, используйте команду debug mac
- **сообщение debug dhcp включает** — для настройки отладки сообщений об ошибках DHCP

Это примеры выходных данных от **команды debug dot1x events enable** и **команды debug client <mac address>**.

события debug dot1x включают:

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to mobile
00:40:96:ac:e6:57 (EAP Id 2) Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity
Response (count=2) from mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57
Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007:
00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3) Tue Dec 18
06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3,
EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile
00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
mobile 00:40:96:ac:e6:57 (EAP Id 4) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP
Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25) Tue Dec 18 06:58:51 2007:
00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51
2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5) Tue
Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP
Id 5, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
```

mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 6, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 7) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 7, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 8) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 8, EAP Type 25) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 9) Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 12) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 12, EAP Type 25) Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Processing Access-Accept for mobile 00:40:96:ac:e6:57** Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)** Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 13)** Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending default RC4 key to mobile 00:40:96:ac:e6:57** Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57** Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received Auth Success while in Authenticating state for mobile 00:40:96:ac:e6:57**

адрес debug mac <MAC-адрес>:

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Association received from mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 - rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0 0 0 Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 RUN (20) Change state to START (0)** Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0) Initializing policy** Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0) Change state to AUTHCHECK (2)** Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2) Change state to 8021X_REQD (3)** Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3)** Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of Mobile Station: 00:40:96:ac:e6:57 (callerId: 48) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry. Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Connecting state Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP- Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1)** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAPOL START from mobile 00:40:96:ac:e6:57** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **EAP State update from Connecting to Authenticating for mobile 00:40:96:ac:e6:57** Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Authenticating state** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)** Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=4) for mobile

00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25) Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6) Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25) Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10) Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25) Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Processing Access-Accept for mobile 00:40:96:ac:e6:57** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Sending default RC4 key to mobile 00:40:96:ac:e6:57** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3) **Change state to L2AUTHCOMPLETE (4)** Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 L2AUTHCOMPLETE (4) Change state to RUN (20) Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20) Reached PLUMBFASTPATH: from line 4041 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20) Replacing Fast Path rule type = Airespace AP Client on AP 00:0b:85:51:5a:e0, slot 0, interface = 2 ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20) Card = 0 (slot 0), InHandle = 0x00000000, OutHandle = 0x00000000, npuCryptoFlag = 0x0000 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20) Successfully plumbed mobile rule (ACL ID 255) Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20) Reached RETURN: from line 4041 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend Auth Success state (id=12) for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 **Received Auth Success** while in Authenticating state for mobile 00:40:96:ac:e6:57 Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x - moving mobile **00:40:96:ac:e6:57 into Authenticated state**

Примечание: При использовании Microsoft supplicant для аутентификации с Cisco Secure ACS для аутентификации PEAP, клиент потенциально не аутентифицируется успешно. Иногда первоначальное подключение может аутентифицироваться успешно, но последующие попытки аутентификации быстрого подключения не соединяются успешно. Это - известная неполадка. Подробные данные этой проблемы и исправления для того же доступны здесь.

Дополнительные сведения

- PEAP в единой беспроводной сети с ACS 4.0 и Windows 2004
- Пример конфигурации аутентификации EAP в контроллерах WLAN (WLC)

- Обновление программного обеспечения контроллера беспроводной локальной сети (WLC) к версиям 3.2, 4.0, и 4.1
- Руководства по конфигурации контроллеров беспроводной локальной сети Cisco серии 4400
- Cisco Systems – техническая поддержка и документация