NPS, контроллеры беспроводной локальной сети и пример конфигурации беспроводных сетей

Содержание

Введение

Этот документ предоставляет пример конфигурации для Защищенного расширяемого протокола аутентификации (PEAP) с Протоколом квитирования с аутентификацией Microsoft (MS-CHAP) аутентификация версии 2 в единой беспроводной сети Cisco (UWN) с Сервером политик сети Microsoft (NPS) как сервер RADIUS.

Предварительные условия

Требования

Гарантируйте, что вы знакомы с этими процедурами перед попыткой этой конфигурации:

- Установка Windows 2008 знания основ

- Знание установки контроллера Cisco

Гарантируйте, что эти требования были удовлетворены перед попыткой этой конфигурации:

- Установите операционную систему Microsoft Windows server 2008 года на каждом из серверов в тестовой лабораторной работе.
- Обновите все пакеты обновления.
- Установите контроллеры и облегченные точки доступа (LAP).
- Настройте обновления последних версий программного обеспечения.

Для начальной установки и сведений о конфигурации для Cisco Контроллеры беспроводной локальной сети серии 5508, обратитесь к Руководству по установке контроллера беспроводной локальной сети Cisco серии 5500.

Примечание: Этот документ предназначен, чтобы дать читателям пример на конфигурации, требуемой на сервере Microsoft для аутентификации PEAP-MS-CHAP. Конфигурация Microsoft Windows server, представленная в этом документе, была протестирована в лабораторной работе и, как находили, работала как ожидалось. Если вы испытываете затруднения из-за конфигурации, свяжитесь с Microsoft для справки. Центр технической поддержки Cisco (TAC) не поддерживает конфигурацию Microsoft Windows server.

Установка Microsoft Windows 2008 года и руководства по конфигурации могут быть найдены на Microsoft Tech Net.

Используемые компоненты

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

- Контроллер беспроводной локальной сети Cisco 5508, который выполняет версию микропрограммы 7.4
- Cisco Aironet 3602 точки доступа (AP) с протоколом LWAPP
- Windows 2008 Enterprise Server с NPS, Центром сертификации (CA), протоколом управления динамическими узлами (DHCP) (DHCP) и сервисами Системы доменных имен (DNS) установлен
- Microsoft Windows 7 клиентских компьютеров
- Коммутатор Cisco Catalyst серии 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 NPS или любой сервер RADIUS. PEAP не задает метод аутентификации, но предоставляет дополнительные меры безопасности для других Расширяемых протоколов аутентификации (EAPs), таких как MS-CHAP EAP v2, который может работать через зашифрованный TLS канал, предоставленный PEAP. Процесс аутентификации PEAP состоит из двух основных этапов.

Фаза 1 PEAP: зашифрованный TLS 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. 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 NPS, о сеансе TLS выполняют согласование между клиентом и NPS. 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. NPS аутентифицирует беспроводного клиента с MS-CHAP EAP v2. LAP и контроллер только передают сообщения между беспроводным клиентом и сервером RADIUS. Контроллер беспроводной локальной сети (WLC) и LAP не могут дешифровать эти сообщения, потому что это не оконечная точка TLS.

Последовательность Сообщения RADIUS для попытки успешной аутентификации (где пользователь предоставил основанные на правильном пароле учетные данные PEAP-MS-CHAP v2) :

1. NPS передает идентификационное сообщение запроса клиенту: `EAP-Request/Identity`.
2. Клиент отвечает идентификационным ответным сообщением: `EAP-Response/Identity`.
3. NPS 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, NPS 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. NPS передает EAP-type-length-value (TLV), 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 в открытом тексте. Если VLAN развернуты для клиентской изоляции, атрибуты VLAN включены в это сообщение.

Настройка

В этом разделе вам предоставляют информацию по настройке 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

Данная конфигурация использует следующую настройку сети:

В этой настройке сервер Microsoft Windows 2008 выполняет эти роли:

- Контроллер домена для домена wireless.com
- DHCP/СЕРВЕР DNS
- CA сервер
- NPS? аутентифицировать пользователей беспроводной связи
- Active Directory? поддерживать базу данных пользователей

Сервер соединяется с проводной сетью через Коммутатор уровня 2 как показано. WLC и зарегистрированный LAP также соединяются с сетью через Коммутатор уровня 2.

Беспроводные клиенты используют Защищенный доступ по протоколу Wi-Fi 2 (WPA2) - аутентификация PEAP-MS-CHAP v2 для соединения с беспроводной сетью.

Конфигурации

Цель данного примера состоит в том, чтобы настроить сервер Microsoft 2008, Контроллер беспроводной локальной сети и AP Легкого веса для аутентификации беспроводных клиентов с аутентификацией PEAP-MS-CHAP v2. В этом процессе существует три главных действия:

1. Настройте Microsoft Windows 2008 Server.
2. Настройте WLC и AP легкого веса.
3. Настройте беспроводных клиентов.

Настройте Microsoft Windows 2008 Server

В данном примере завершенная конфигурация сервера Microsoft Windows 2008 включает эти шаги:

1. Настройте сервер как контроллер домена.
2. Установите и настройте сервисы DHCP.
3. установите и настройте сервер как сервер CA.

4. Подключите клиентов с доменом.
5. Установите NPS.
6. Установите сертификат.
7. Настройте NPS для аутентификации PEAP.
8. Добавьте пользователей к Active Directory.

Настройте Microsoft Windows 2008 Server как контроллер домена

Выполните эти шаги для настройки сервера Microsoft Windows 2008 как контроллера домена:

1. Нажмите **Start > Server Manager**.

2. Нажмите **Roles > Add Roles**.

3. **Нажмите кнопку Next.**

4. Выберите сервисные **Доменные сервисы Active Directory** и нажмите **Next**.

5. Рассмотрите Введение к Доменным сервисам Active Directory и нажмите **Next**.

6. Нажмите **Install** для начала процесса установки.

   Установка продолжается и завершает.

7. Нажмите **Close этот мастер и запустите Мастера установки доменных служб Active Directory (dcpromo.exe)** для продолжения установки и конфигурации Active Directory.

8. Нажмите **Next** для выполнения Мастера установки доменных служб Active Directory.

9. Рассмотрите информацию об Операционной системе Compatbilty и нажмите **Next**.

10. Нажмите **Create новый домен в новом лесу> Затем** для создания нового домена.

11. Введите полное имя DNS для нового домена (wireless.com в данном примере) и нажмите **Next**.

12. Выберите лесной функциональный уровень для своего домена и нажмите **Next**.

13. Выберите доменный функциональный уровень для своего домена и нажмите **Next**.

14. Гарантируйте, что сервер DNS выбран, и нажмите **Next**.

15. Нажмите **Yes** для мастера установки для создания новой зоны в DNS для домена.

16. Выберите папки Active Directory, должен использовать для его файлов и нажать **Next**.

17. Введите Пароль администратора и нажмите **Next**.

18. Рассмотрите свои выборы и нажмите **Next**.

    Доходы установки.

19. Нажмите **Finish** для закрытия мастера.

20. Перезапустите сервер для изменений для вступления в силу.

Установите и настройте сервисы DHCP на Microsoft Windows 2008 Server

Сервис DHCP на сервере Microsoft 2008 используется для обеспечения IP-адресов беспроводным клиентам. Выполните эти шаги, чтобы установить и настроить сервисы DHCP:

1. Нажмите **Start > Server Manager**.

2. Нажмите **Roles > Add Roles**.

3. **Нажмите кнопку Next.**

4. Выберите **Сервер service DHCP** и нажмите **Next**.

5. Рассмотрите Введение к Серверу DHCP и нажмите **Next**.

6. Выберите интерфейс, который сервер DHCP должен контролировать для запросов, и нажимать **Next**.

7. Настройте параметры настройки DNS по умолчанию, которые сервер DHCP должен предоставить клиентам и нажать **Next**.

8. Настройте WINS, если сеть поддерживает WINS.

9. **Нажмите Add** для использования мастера, чтобы создать Область DHCP или нажать **Next** для создания области DHCP позже. **Для продолжения щелкните кнопку "Далее".**

10. Включите или отключите поддержку DHCPv6 на сервере и нажмите **Next**.

11. Настройте параметры настройки DNS IPv6, если DHCPv6 был включен в предыдущем шаге. **Для продолжения щелкните кнопку "Далее".**

12. Предоставьте учетные данные администратора домена, чтобы авторизовать сервер DHCP в Active Directory и нажать **Next**.

13. Рассмотрите конфигурацию на странице подтверждения и нажмите **Install** для завершения установки.

    Доходы установки.

14. Нажмите **Close to** закрывают мастера.

    Сервер DHCP теперь установлен.

15. Нажмите **Start> Administrative Tools > DHCP** для настройки сервиса DHCP.

16. Разверните сервер DHCP (победа-mvz9z2umms.wireless.com в данном примере), щелкните правой кнопкой мыши IPv4 и выберите **New Scope**. создать Область DHCP.

17. Нажмите **Next** для настройки новой области через Нового Мастера создания области.

18. Предоставьте название для новой области (Беспроводные клиенты в данном примере) и нажмите **Next**.

19. Введите диапазон доступных IP-адресов, которые могут использоваться для аренды DHCP. **Для продолжения щелкните кнопку "Далее".**

20. Создайте дополнительный список исключенных адресов. **Для продолжения щелкните кнопку "Далее".**

21. Настройте время аренды и нажмите **Next**.

22. **Нажмите кнопку Да, я хочу настроить эти опции теперь** и нажать **Next**.

23. Введите IP-адрес шлюза по умолчанию для этой области, **нажмите Add > Затем**.

24. Настройте название Домена DNS и сервер DNS, который будет использоваться клиентами. **Для продолжения щелкните кнопку "Далее".**

25. Введите информацию о WINS для этой области, если сеть поддерживает WINS. **Для продолжения щелкните кнопку "Далее".**

26. Для активации этой области **нажмите кнопку Да, я хочу активировать эту область теперь > Затем**.

27. Нажмите **Finish**, чтобы завершить и закрыть мастера.

Установите и настройте Microsoft Windows 2008 Server как сервер CA

PEAP с MS-CHAP EAP v2 проверяет сервер RADIUS на основе подарка сертификата на сервере. Кроме того, серверный сертификат должен быть выполнен общественностью CA, которой доверяет компьютер клиента (т.е. общий сертификат CA уже существует в папке Trusted Root Certification Authority на хранилище сертификата компьютера клиента).

Выполните эти шаги для настройки сервера Microsoft Windows 2008 как сервера CA, который выполняет сертификат к NPS:

1. Нажмите **Start > Server Manager**.

2. Нажмите **Roles > Add Roles**.

3. **Нажмите кнопку Next.**

4. Выберите сервисные **Сервисы сертификации Active Directory** и нажмите **Next**.

5. Рассмотрите Введение к Сервисам сертификации Active Directory и нажмите **Next**.

6. Выберите **Certificate Authority** и нажмите **Next**.

7. Выберите **Enterprise** и нажмите **Next**.

8. Выберите **Root CA** и нажмите **Next**.

9. Выберите **Create новый секретный ключ** и нажмите **Next**.

10. Нажмите **Next on Configuring Cryptography for CA.**

11. Нажмите **Next** для принятия Общего имени по умолчанию для этого CA.

12. Выберите промежуток времени, этот сертификат CA допустим, и нажмите **Next**.

13. Нажмите **Next** для принятия расположения базы данных Сертификата по умолчанию.

14. Рассмотрите конфигурацию и нажмите **Install** для начала Сервисов сертификации Active Directory.

15. После того, как установка завершена, нажмите **Close**.

Подключите клиентов с доменом

Выполните эти шаги для подключения клиентов с проводной сетью и загружать зависящую от домена информацию от нового домена:

1. Подключите клиентов с проводной сетью со сквозным Кабелем Ethernet.
2. Загрузите клиента и войдите с клиентским именем пользователя и паролем.
3. Нажмите **Start> Run** , введите **cmd** и нажмите **OK**.
4. В командной строке введите **ipconfig** и нажмите **Enter**, чтобы проверить, что DHCP работает правильно и что клиент получил IP-адрес от сервера DHCP.
5. Для соединения клиента с доменом нажмите **Start**, щелкните правой кнопкой мыши **Компьютер**, выберите **Properties** и выберите **Change Settings** в нижнем правом угле.
6. **Нажмите кнопку «Изменить».**
7. Нажмите **Domain**, введите **wireless.com** и нажмите **OK**.

8. Введите **администратора** имени пользователя и пароль, определенный для домена, к которому присоединяется клиент. Это - учетная запись администратора в Active Directory на сервере.

9. **Нажмите OK** и нажмите **OK** снова.

10. Нажмите **Close > Restart Now** для перезапуска компьютера.
11. Как только компьютер перезапускает, войдите с этой информацией: Имя пользователя = Администратор; Пароль = <пароль домена>; Домен = радио.
12. Нажмите **Start**, щелкните правой кнопкой мыши **Компьютер**, выберите **Properties** и выберите **Change Settings** в нижнем правом угле, чтобы проверить, что вы находитесь на wireless.com домене.
13. Следующий шаг должен проверить, что клиент получил сертификат CA (доверие) от сервера.

14. Нажмите **Start**, введите **mmc** и нажмите **Enter**.

15. Нажмите **File** и нажмите моментальный снимок **Add/Remove** - в.
16. **Выберите Certificates (Сертификаты) и нажмите кнопку Add (Добавить).**

17. Нажмите **Учетную запись компьютера** и нажмите **Next**.

18. Нажмите **Локальный компьютер** и нажмите **Next**.

19. **Нажмите кнопку OK.**
20. Разверните папки **Certificates (Local Computer) и Trusted Root Certification Authorities** и нажмите **Certificates**. Найдите **домен беспроводной связи CA свидетельством** в списке. В данном примере свидетельство CA называют wireless-WIN-MVZ9Z2UMNMS-CA.

21. Повторите эту процедуру для добавления большего количества клиентов к домену.

Установите сервер сетевой политики на Microsoft Windows 2008 Server

В этой настройке NPS используется в качестве сервера RADIUS для аутентификации беспроводных клиентов с аутентификацией PEAP. Выполните эти шаги, чтобы установить и настроить NPS на сервере Microsoft Windows 2008:

1. Нажмите **Start > Server Manager**.

2. Нажмите **Roles > Add Roles**.

3. **Нажмите кнопку Next.**

4. Выберите **сеть услуг Политика и Службы доступа**, и нажмите **Next**.

5. Рассмотрите Введение к Сетевой политике и Службам доступа, и нажмите **Next**.

6. Выберите **Network Policy Server** и нажмите **Next**.

7. Рассмотрите подтверждение и нажмите **Install**.

   После того, как установка завершена, экран, подобный этому, отображен.

8. **Нажмите кнопку Закрыть.**

Установите сертификат

Выполните эти шаги для установки компьютерного сертификата для NPS:

1. Нажмите **Start**, введите **mmc** и нажмите **Enter**.
2. Нажмите **File> Add/Remove Snap - в**.
3. **Выберите Certificates (Сертификаты) и нажмите кнопку Add (Добавить).**

4. Выберите **Учетную запись компьютера** и нажмите **Next**.

5. Выберите **Local Computer** и нажмите **Finish**.

6. Нажмите **OK** для возврата к Консоли управления Microsoft (MMC).

7. Разверните **Сертификаты (Локальный компьютер)** и **Персональные папки** , и нажмите **Certificates**.

8. Щелкните правой кнопкой мыши в пробеле ниже сертификата CA и выберите **All Tasks> Request New Certificate**.

9. **Нажмите кнопку Next.**

10. Выберите **Domain Controller** и нажмите **Enroll**.

11. Нажмите **Finish**, как только установлен сертификат.

    Сертификат NPS теперь установлен.

12. Гарантируйте, что Намеченная Цель сертификата читает **Аутентификацию клиента, Проверку подлинности сервера**.

Настройте Сервис сервера Сетевой политики для Аутентификации PEAP-MS-CHAP v2

Выполните эти шаги для настройки NPS для аутентификации:

1. Нажмите **Start> Administrative Tools** > **Network Policy Server**.
2. Щелкните правой кнопкой мыши **(Локального) NPS**, и выберите **сервер Register в Active Directory**.

3. **Нажмите кнопку ОК.**

4. **Нажмите кнопку ОК.**

5. Добавьте Контроллер беспроводной локальной сети как клиента аутентификации, авторизации и учета (AAA) на NPS.
6. Разверните **Клиентов RADIUS и Серверы**. Щелкните правой кнопкой мыши **Клиентов RADIUS** и выберите **New RADIUS Client**.

7. Введите Дружественное имя (WLC в данном примере), управление IP-адресами WLC (192.168.162.248 в данном примере) и общий секретный ключ. Тот же общий секретный ключ используется для настройки WLC.

8. Нажмите **OK** для возврата к предыдущему экрану.

9. Создайте новую Сетевую политику для пользователей беспроводной связи. Разверните **Политику**, щелкните правой кнопкой мыши **Сетевую политику** и выберите **New**.

10. Введите имя политики для этого правила (Беспроводной PEAP в данном примере) и нажмите **Next**.

11. Для имения этой политики позволяют только пользователям домена беспроводной связи добавляют, эти три условия и нажимают **Next**:

    - Windows Groups - Пользователи домена
    - Тип порта NAS - беспроводные сети - IEEE 802.11
    - Тип проверки подлинности - EAP

12. Нажмите **Access предоставил** предоставлять попытки подключения, которые совпадают с этой политикой и нажимают **Next**.

13. Отключите все методы аутентификации в соответствии с Меньшим количеством методов безопасной аутентификации.

14. **Нажмите Add**, выберите PEAP и нажмите **OK** для включения PEAP.

15. Выберите **Microsoft: Защищенный EAP (PEAP)**, и нажимает **Edit**. Гарантируйте, что ранее созданный сертификат контроллера домена выбран в выполненном выпадающем списке Сертификата, и нажмите **Ok**.

16. **Нажмите кнопку Next.**

17. **Нажмите кнопку Next.**

18. **Нажмите кнопку Next.**

19. **Нажмите кнопку Finish.**

Добавьте пользователей к Active Directory

В данном примере база данных пользователей поддержана на Active Directory. Выполните эти шаги для добавления пользователей к базе данных Active Directory:

1. Откройте службу Active Directory Users and Computers. Нажмите **Start> Administrative Tools > Active Directory Users and Computers**.
2. В дереве консоли Пользователей и компьютеров Active Directory разверните домен, щелкните правой кнопкой мыши **Пользователей > Новый**, и выберите **User**.
3. В Новом Объекте? Диалоговое окно User, введите имя пользователя беспроводной связи. Данный пример использует название Client1 в поле Имени и Client1 в Пользовательском поле имени пользователя. **Нажмите кнопку Next.**

4. В Новом Объекте? Диалоговое окно User, введите пароль по Вашему выбору в Полях Password и Полях подтверждения пароля. Анчек **Пользователь должен изменить пароль в следующем** флажке **входа в систему** и нажать **Next**.

5. В Новом Объекте? Диалоговое окно User, нажмите **Finish**.

6. Повторите шаги 2 - 4 для создания дополнительных учетных записей пользователя.

Настройте контроллер беспроводной локальной сети и LAP

Настройте беспроводные устройства (Контроллеры беспроводной локальной сети и LAP) для этой настройки.

Настройте WLC для проверки подлинности RADIUS

Настройте WLC для использования NPS в качестве сервера проверки подлинности. WLC должен быть настроен для передачи учетных данных пользователя внешнему серверу

RADIUS. Внешний сервер RADIUS проверяет учетные данные пользователя и предоставляет доступ беспроводным клиентам.

Выполните эти шаги для добавления NPS как сервера RADIUS на странице **Security> RADIUS Authentication**:

1. Выберите **Security > RADIUS> Authentication** от интерфейса контроллера для отображения страницы RADIUS Authentication Servers. Нажмите **New** для определения сервера RADIUS.

2. Определите параметры сервера RADIUS. В их числе: RADIUS Server IP Address, Shared Secret, Port Number и Server Status. Флажки Network User и Management определяют, применяется ли основанная на RADIUS аутентификация к управлению и сетевым (беспроводным) пользователям. Данный пример использует NPS в качестве сервера RADIUS с IP-адресом 192.168.162.12. **Щелкните "Применить".**

Настройте WLAN для клиентов

Настройте набор сервисов identfier (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 основанную на EAP аутентификацию (PEAP-MS-CHAP v2 в данном примере) и использовали расширенный стандарт шифрования (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.

Выполните эти шаги для настройки WLAN на WLC:

1. Нажмите **WLAN** от интерфейса контроллера для отображения страницы 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. Для настройки SSID для 802.1x выполните эти шаги: Нажмите **Вкладку Общие** и включите WLAN.

   Нажмите **Безопасность> Таблицы уровня 2**, установите безопасность уровня 2 в **WPA + WPA2**, проверьте, что Параметры WPA+WPA2 (например, AES WPA2) проверяют

boxesas, необходимый, и **802.1x** щелчка как менеджмент Ключа проверки подлинности.

Нажмите вкладки **Security> AAA Servers**, выберите IP-адрес NPS от **Сервера 1** выпадающий список и нажмите **Apply**.

Настройте Беспроводных клиентов для Аутентификации PEAP-MS-CHAP v2

Выполните эти шаги для настройки беспроводного клиента с Windows Zero Config Tool для соединения с WLAN PEAP.

1. Нажмите **Значок сети** в панели задач. Нажмите **PEAP SSID** и нажмите **Connect**.

2. Клиент должен теперь быть связан с сетью.

3. Если связь прерывается, попытайтесь воссоединиться с WLAN. Если проблема сохраняется, обратитесь к разделу Устранения неполадок.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Если ваш клиент не соединился с WLAN, этот раздел предоставляет сведения, можно использовать для устранения проблем конфигурации.

Существует два программных средства, которые могут использоваться для диагностирования ошибок проверки подлинности 802.1x: **команда debug client** и **Просмотр событий** в Windows.

Выполнение клиентской отладки от WLC не является потребляющими ресурсами и не делает imnpact сервиса. Для начала сеанса отладки откройте интерфейс командной строки (CLI) WLC и введите *мак адрес* **клиента отладки**, где мак адрес является беспроводным мак адресом беспроводного клиента, который неспособен соединиться. В то время как эта отладка выполняется, попытайтесь подключить клиента; там должен быть выведен на CLI WLC, который выглядит подобным данному примеру:

Это - пример проблемы, которая могла произойти с неверной конфигурацией. Здесь, отладка WLC показывает, что WLC переместился в аутентифицирующееся состояние, что

означает, что WLC ждет ответа от NPS. Это обычно происходит из-за неправильного общего секретного ключа или на WLC или на NPS. Можно подтвердить это через Просмотр событий Windows Server. Если вы не находите журнал, запрос никогда не добирался до NPS.

Другим примером, который найден от отладки WLC, является отклонение доступа. Отклонение доступа показывает, что NPS получил и отклонил удостоверения клиента. Это - пример клиента, получающего отклонение доступа:

Когда вы видите отклонение доступа, проверьте вход в систему Журналов событий Windows Server для определения, почему NPS ответил клиенту с отклонением доступа.

Успешная аутентификация имеет access-accept в клиентской отладке, как замечено в данном примере:

Устранение проблем отклонений доступа и времен ожидания ответа требует доступа к серверу RADIUS. WLC действует как средство проверки подлинности, которое передает сообщения EAP между клиентом и сервером RADIUS. Сервер RADIUS, отвечающий отклонением доступа или временем ожидания ответа, должен быть исследован и диагностирован изготовителем Сервиса RADIUS.

Примечание: TAC не предоставляет техническую поддержку для сторонних серверов RADIUS; однако, вход в систему сервера RADIUS обычно объясняет, почему запрос клиента был отклонен или проигнорирован.

Для устранения проблем отклонений доступа и времен ожидания ответа от NPS, исследуйте NPS, входит в Windows Event Viewer на сервере.

1. Нажмите **Start> Administrator Tools> Event Viewer** , чтобы запустить Просмотр событий и рассмотреть журналы NPS.
2. Разверните **Пользовательские Представления> Роли сервера> Сетевая политика и Доступ**.

В этом разделе События View существуют журналы переданных и ошибок проверки подлинности. Исследуйте эти журналы для устранения проблем, почему клиент не передает аутентификацию. Оба прошли, и ошибки проверки подлинности обнаруживаются как Информационные. Просмотрите журналы путем прокрутки для обнаружения имени пользователя, которое имеет ошибку проверки подлинности и получило отклонение доступа согласно отладкам WLC.

Это - пример NPS, запрещающего пользовательский доступ:

При рассмотрении инструкции deny в конечном счете Средство просмотра, исследуйте Опознавательный Подробный раздел. В данном примере вы видите, что NPS запретил пользовательский доступ из-за неверного имени пользователя:

Если WLC не получает ответ назад от NPS, Событие View на NPS также помогает с устранением проблем. Это обычно вызывается неправильным общим секретным ключом

между NPS и WLC.

В данном примере NPS сбрасывает от запроса от WLC из-за неправильного общего секретного ключа:

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация