Аутентификация PEAP WLC Серии 5760/3850 с Microsoft NPS Configuration Example

ID документа: 117684

Обновлено : 05 мая 2014

Внесенный BG Surendra, специалистом службы технической поддержки Cisco.

Родственные продукты

- Cisco контроллеры беспроводной локальной сети серии 5700
- Служба удаленной аутентификации пользователей коммутируемого доступа (RADIUS)

Содержание

Введение

Этот документ описывает, как настроить Защищенный расширяемый протокол аутентификации (PEAP) с Версией протокола 2 квитирования с аутентификацией Microsoft (MS-CHAP v2) аутентификация на Cisco Сходившаяся Беспроводная локальная сеть Доступа (WLAN) развертывания с Сервером политик сети Microsoft (NPS) как сервер RADIUS.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с этими темами перед попыткой конфигурации, описанной в этом документе:

- Основная установка Версии 2008 Microsoft Windows
- Cisco Сходилась установка контроллера беспроводной локальной сети Доступа

Гарантируйте, что эти требования удовлетворены перед попыткой этой конфигурации:

- Установите Операционную систему (OS) Версии 2008 Microsoft Windows server 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.

Примечание: Поскольку начальная установка и сведения о конфигурации для Cisco Сходились контроллеры беспроводной локальной сети Доступа, обратитесь к статье CT5760 Controller и Catalyst 3850 Switch Configuration Example Cisco.

Используемые компоненты

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

- Cisco версия 3.3.2 контроллера беспроводной локальной сети серии 5760 (Коммутационный шкаф следующего поколения (NGWC))
- Cisco LAP серии 3602
- Microsoft Windows XP с Intel соискатель PROset
- Сервер Версии 2008 Microsoft Windows, который выполняет NPS с Ролями Контроллера домена
- 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.

Общие сведения

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, который предоставлен PEAP. Процесс аутентификации PEAP состоит из двух основных этапов.

Фаза 1 PEAP: зашифрованный TLS канал

Беспроводной клиент связывается с Точкой доступа (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 AP. После того, как основанная на IEEE 802.11 ассоциация успешно установлена между клиентом и AP, 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, который создан 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 может дешифровать сообщения, потому что WLC не является оконечной точкой TLS.

Вот последовательность Сообщения RADIUS для попытки успешной аутентификации, где пользователь предоставляет 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 MS-CHAP-V2 (Challenge)`
4. Клиент отвечает проблемой MS-CHAP v2 и ответом:
   `EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response)`
5. Когда сервер успешно аутентифицирует клиента, NPS отвечает пакетом MS-CHAP v2 успеха:
   `EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success)`
6. Когда клиент успешно аутентифицирует сервер, клиент отвечает пакетом MS-CHAP v2 успеха:
   `EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success)`
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

Используйте этот раздел для настройки PEAP с аутентификацией MS-CHAP v2 на Cisco Сходившиеся развертывания WLC Доступа с Microsoft NPS как сервер RADIUS.

Схема сети

В данном примере сервер Версии 2008 Microsoft Windows выполняет эти роли:

- Контроллер домена для **wireless.com** домена
- Сервер Системы доменных имен (DNS)
- Сервер Центра сертификации (CA)
- NPS для аутентификации пользователей беспроводной связи
- Active Directory (AD) для поддержания базы данных пользователей

Сервер подключает с проводной сетью через Уровень 2 (L2) коммутатор, как показано. WLC и зарегистрированный LAP также соединяются с сетью через коммутатор L2.

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

Конфигурации

Конфигурация, которая описана в этом разделе, завершена в двух шагах:

1. Настройте 5760/3850 WLC Серии с CLI или GUI.

2. Настройте сервер Версии 2008 Microsoft Windows для NPS, Контроллера домена и Учетных записей пользователя на AD.

Настройте сходившиеся WLC доступа с CLI

Выполните эти шаги, чтобы настроить WLAN для требуемой клиентской VLAN и сопоставить его со Списком способов аутентификации с CLI:

> **Примечание:** Гарантируйте, что **системный контроль за аутентификацией dot1x** включен на WLC, или dot1X не работает.

1. Активируйте опцию **новой модели AAA**.

2. Настройка RADIUS-сервера.

3. Добавьте сервер в Группу серверов.

4. Сопоставьте группу серверов со списком методов.

5. Сопоставьте список методов с WLAN.

```
aaa new-model
!
!
aaa group server radius Microsoft_NPS
 server name Microsoft_NPS
!
aaa authentication dot1x Microsoft_NPS group Microsoft_NPSaaa authorization network
Microsoft_NPS group Microsoft_NPS
radius server Microsoft_NPS
 address ipv4 10.104.208.96 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 10
 key Cisco123wlan Microsoft_NPS 8 Microsoft_NPS
 client vlan VLAN0020
 no exclusionlist
 security dot1x authentication-list Microsoft_NPS
 session-timeout 1800
 no shutdown
```

Настройте сходившиеся WLC доступа с GUI

Выполните эти шаги для настройки Установившихся WLC Доступа с GUI:

1. Включите **dot1x system-auth-control**:

2. Перейдите к**> Security Конфигурации> AAA** для добавления сервера RADIUS:

3. Перейдите к **RADIUS> Серверы**, нажмите **NEW** и обновите IP-адрес сервера RADIUS наряду с общим секретным ключом. Общий секретный ключ должен совпасть с общим секретным ключом, который настроен на сервере RADIUS также.

   После настройки сервера RADIUS вкладка Server должна казаться подобной этому:

4. Настройте Группу серверов и выберите **Radius** для Типа группы. Затем добавьте сервер RADIUS, который вы создали в предыдущем шаге:

Группа серверов должна казаться подобной этому после конфигурации:

5. Выберите **dot1x** для Типа Списка способов аутентификации и **Группу** для Типа группы. Затем сопоставьте Группу серверов, которую вы настроили в предыдущем шаге:

   Список способов аутентификации должен казаться подобным этому после конфигурации:

6. Выберите **Network** для Типа Списка Метода авторизации и **Группу** для Типа группы. Затем сопоставьте Группу серверов, которую вы настроили в предыдущем шаге:

   Список Метода авторизации должен казаться подобным этому после конфигурации:

7. Перейдите, чтобы **Настроить> беспроводные сети** и нажать вкладку **WLAN**. Настройте новый WLAN, с которым пользователи могут соединиться и стать аутентифицируемыми через сервер Microsoft NPS с Аутентификацией eap:

   Вкладка Security L2 должна казаться подобной этому после конфигурации:

8. Сопоставьте Список методов, который вы настроили в предыдущих шагах. Это помогает аутентифицировать клиента на корректном сервере.

Конфигурация на сервере версии 2008 Microsoft Windows

В этом разделе описываются завершенную конфигурацию сервера Версии 2008 Microsoft Windows. Конфигурация завершена в шести шагах:

1. Настройте сервер как контроллер домена.
2. Установите и настройте сервер как сервер CA.
3. Установите NPS.

4. Установите сертификат.

5. Настройте NPS для аутентификации PEAP.

6. Добавьте пользователей к AD.

Настройте Microsoft Windows 2008 Server как контроллер домена

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

1. Перейдите для **Начала > Диспетчер серверов>, Роли > Добавляют Роли**.

2. **Нажмите кнопку Next.**

3. Проверьте флажок **Active Directory Domain Services** и нажмите **Next**.

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

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

   Установка продолжается и завершает.

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

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

8. Рассмотрите информацию о **Совместимости Операционной системы** и нажмите **Next**.

9. Нажмите **Create новый домен в** кнопке с зависимой фиксацией **нового леса** и нажмите **Next** для создания нового домена.

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

11. Выберите **Лесной функциональный уровень** для своего домена и нажмите **Next**.

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

13. Проверьте флажок **сервера DNS** и нажмите **Next**.

14. Нажмите **Yes**, когда всплывающее окно **Active Directory Domain Services Installation Wizard** появляется для создания новой зоны в DNS для домена.

15. Выберите папки, которые вы хотите, чтобы AD использовал для файлов и нажал **Next**.

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

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

    Доходы установки.

18. Нажмите **Finish** для закрытия мастера.

19. Перезапустите сервер для изменений для вступления в силу.

Установите и настройте сервер версии 2008 Microsoft Windows как сервер CA

PEAP с MS-CHAP EAP v2 проверяет сервер RADIUS, основанный на сертификате, который присутствует 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 Версии 2008 Microsoft Windows как сервера CA, который выполняет сертификат к NPS:

1. Перейдите для **Начала > Диспетчер серверов>, Роли > Добавляют Роли**.

2. **Нажмите кнопку Next.**

3. Проверьте флажок **Active Directory Certificate Services** и нажмите **Next**.

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

5. Проверьте флажок **Certificate Authority** и нажмите **Next**.

6. Нажмите кнопку с зависимой фиксацией **Enterprise** и нажмите **Next**.

7. Нажмите кнопку с зависимой фиксацией **Root CA** и нажмите **Next**.

8. Нажмите **Create новая** кнопка с зависимой фиксацией **с закрытым ключом** и нажмите **Next**.

9. Нажмите **Next** в окне **Configuring Cryptography for CA**.

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

11. Выберите промежуток времени, в течение которого сертификат CA допустим, и нажмите **Next**.

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

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

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

Установите NPS на сервере версии 2008 Microsoft Windows

> **Примечание:** С настройкой, которая описана в этом разделе, NPS используется в качестве сервера RADIUS для аутентификации беспроводных клиентов с аутентификацией PEAP.

Выполните эти шаги, чтобы установить и настроить NPS на сервере Версии 2008 Microsoft Windows:

1. Перейдите для **Начала > Диспетчер серверов>, Роли > Добавляют Роли**.

2. **Нажмите кнопку Next.**

3. Проверьте флажок **Network Policy и Access Services** и нажмите **Next**.

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

5. Проверьте **флажок Server Сетевой политики** и нажмите **Next**.

6. Рассмотрите подтверждение и нажмите **Install**.

После того, как установка завершена, экран, подобный этому, должен появиться:

7. **Нажмите кнопку Закрыть.**

Установите сертификат

Выполните эти шаги для установки компьютерного сертификата для NPS:

1. Нажмите **Start**, введите Консоль управления Microsoft (MMC) и нажмите **Enter**.
2. Перейдите к **Файлу>, Добавляет/Удаляет Моментальный снимок - в**.
3. **Выберите Certificates (Сертификаты) и нажмите кнопку Add (Добавить).**
4. Нажмите кнопку с зависимой фиксацией **Учетной записи компьютера** и нажмите **Next**.
5. Нажмите кнопку с зависимой фиксацией **Local Computer** и нажмите **Finish**.
6. Нажмите **OK** для возврата к MMC.
7. Разверните **Сертификаты (Локальный компьютер)** и **Персональные папки** , и нажмите **Certificates**.
8. Щелкните правой кнопкой мыши пробел в сертификате CA и выберите **All Tasks> Request New Certificate**.
9. **Нажмите кнопку Next.**

10. Нажмите флажок **Domain Controller** и нажмите **Enroll**.

    Примечание: Если аутентификация клиента отказывает из-за ошибки сертификата EAP, то гарантируйте, что все флажки проверены на этой странице **Certificate Enrollment** перед нажатием **Enroll**. Это создает приблизительно три сертификата.

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

    Сертификат NPS теперь установлен.

12. Гарантируйте, что **Аутентификация клиента, Проверка подлинности сервера** появляется в столбце Intended Purposes для сертификата.

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

Выполните эти шаги для настройки NPS для аутентификации:

1. Перейдите к **Пуску> Средства администрирования > Сервер Сетевой политики**.
2. Щелкните правой кнопкой мыши **(Локального) NPS** и выберите **сервер Register в Active Directory**.
3. **Нажмите кнопку ОК.**
4. **Нажмите кнопку ОК.**
5. Добавьте WLC 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 имя (**WLC** в данном примере), управление IP-адресами WLC (**10.105.135.178** в данном примере), и общий секретный ключ.

    Примечание: 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 (**PEAP** в данном примере) и нажмите **Next**.

11. Для настройки этой политики, чтобы позволить только пользователям домена беспроводной связи, добавьте эти три условия и нажмите **Next**:

12. Нажмите **доступ**, предоставленный кнопка с зависимой фиксацией для предоставления попыток подключения, которые совпадают с этой политикой и нажимают **Next**.

13. Отключите все **Меньше методов безопасной аутентификации**:

14. **Нажмите Add**, выберите **Microsoft: Защищенный EAP (PEAP)**, Тип EAP, и нажимает **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.**

Примечание: Зависящий от ваших потребностей, вы, возможно, должны были бы настроить **Политику Запроса подключения** по NPS для разрешения профиля PEAP или политики.

Добавьте пользователей к Active Directory

Примечание: В данном примере база данных пользователей поддержана на AD.

Выполните эти шаги для добавления пользователей к AD базе данных:

1. Перейдите к **Пуску> Средства администрирования > Пользователи и компьютеры Active Directory**.
2. В дереве консоли Пользователей и компьютеров Active Directory разверните домен, щелкните правой кнопкой мыши **Пользователей** и **Новый**, и выберите **User**.
3. В Новом Объекте - диалоговое окно User, введите имя пользователя беспроводной связи. Данный пример использует **Client1** в поле First Name 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.

Проверка

Выполните эти шаги для проверки конфигурации:

1. Ищите Идентификацию Набора сервисов (SSID) на клиентском компьютере.

2. Гарантируйте, что клиент связан успешно:

Устранение неполадок

> **Примечание:** Cisco рекомендует использовать трассировки для решения беспроводных проблем. Трассировки сохранены в кольцевом буфере и не являются сом интенсивной загрузкой процессора.

Разрешите эти трассировки для получения **подлинных журналов L2**:

- **set trace group-wireless-secure отладка уровня**
- **set trace group-wireless-secure фильтрует mac 0017.7C2F.B69A**

Разрешите эти трассировки для получения **событий AAA dot1X**:

- **отладка уровня aaa wcm-dot1x set trace**
- **aaa wcm-dot1x set trace фильтрует mac 0017.7C2F.B69A**

Разрешите эти трассировки для получения **событий DHCP**:

- **отладка уровня событий dhcp set trace**
- **события dhcp set trace фильтруют mac 0017.7C2F.B69A**

Разрешите эти трассировки, чтобы отключить трассировки и очистить буфер:

- **контроль за set trace sys-filtered-traces ясный**
- **по умолчанию уровня aaa wcm-dot1x set trace**
- **aaa wcm-dot1x set trace не фильтрует ни один**
- **set trace group-wireless-secure по умолчанию уровня**
- **set trace group-wireless-secure не фильтрует ни один**

Введите **show trace sys-filtered-traces** команда для просмотра трассировок:

```
[04/23/14 21:27:51.963 IST 1 8151] 0017.7c2f.b69a Adding mobile on LWAPP AP
 1caa.076f.9e10 (0)
[04/23/14 21:27:51.963 IST 2 8151] 0017.7c2f.b69a Local Policy: Created MSCB
 Just AccessVLAN = 0 and SessionTimeout is 0 and apfMsTimeout is 0

[04/23/14 21:27:51.963 IST 8 8151] 0017.7c2f.b69a Local Policy:Setting local
 bridging VLAN name VLAN0020 and VLAN ID 20

[04/23/14 21:27:51.963 IST 9 8151] 0017.7c2f.b69a Applying WLAN ACL policies
 to client
[04/23/14 21:27:51.963 IST a 8151] 0017.7c2f.b69a No Interface ACL used for
 Wireless client in WCM(NGWC)
[04/23/14 21:27:51.963 IST b 8151] 0017.7c2f.b69a Applying site-specific IPv6
 override for station 0017.7c2f.b69a - vapId 8, site 'test',
 interface 'VLAN0020'
[04/23/14 21:27:51.963 IST c 8151] 0017.7c2f.b69a Applying local bridging
 Interface Policy for station 0017.7c2f.b69a - vlan 20,
```

```
 interface 'VLAN0020'
[04/23/14 21:27:51.963 IST d 8151] 0017.7c2f.b69a
 **** Inside applyLocalProfilingPolicyAction ****

04/23/14 21:27:51.963 IST f 8151] 0017.7c2f.b69a    Local Profiling Values :
 isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
 sessionTimeout=0, isSessionTORecdInDelete = 0 ProtocolMap = 0 ,
 applyPolicyAtRun= 0
[04/23/14 21:27:51.963 IST 10 8151] 0017.7c2f.b69a         ipv4ACL = [],
 ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[04/23/14 21:27:51.963 IST 11 8151] 0017.7c2f.b69a STA - rates (4):
 130 132 139 150 0 0 0 0 0 0 0 0 0 0 0 0
[04/23/14 21:27:51.963 IST 12 8151] 0017.7c2f.b69a STA - rates (12):
 130 132 139 150 12 18 24 36 48 72 96 108 0 0 0 0
[04/23/14 21:27:51.963 IST 13 8151] 0017.7c2f.b69a Processing RSN IE type 48,
 length 20 for mobile 0017.7c2f.b69a
[04/23/14 21:27:51.963 IST 14 8151] 0017.7c2f.b69a Received RSN IE with 0
 PMKIDsfrom mobile 0017.7c2f.b69a


[04/23/14 21:27:51.964 IST 1b 8151] 0017.7c2f.b69a Change state to AUTHCHECK
 (2) last state START (0)

[04/23/14 21:27:51.964 IST 1c 8151] 0017.7c2f.b69a Change state to 8021X_REQD
 (3) last state AUTHCHECK (2)


[04/23/14 21:27:51.964 IST 25 8151] 0017.7c2f.b69a apfProcessAssocReq
 (apf_80211.c:6272) Changing state for mobile 0017.7c2f.b69a on AP
 1caa.076f.9e10 from Associated to Associated

[04/23/14 21:27:51.971 IST 26 8151] 0017.7c2f.b69a 1XA: Initiating
 authentication
[04/23/14 21:27:51.971 IST 27 8151] 0017.7c2f.b69a 1XA: Setting reauth
 timeout to 1800 seconds
[04/23/14 21:27:51.971 IST 28 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 0

[04/23/14 21:27:51.971 IST 29 8151] 0017.7c2f.b69a 1XA: Allocated uid 40
[04/23/14 21:27:51.971 IST 2a 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr
 to authenticate client 4975000000003e uid 40
[04/23/14 21:27:51.971 IST 2b 8151] 0017.7c2f.b69a 1XA: Session Start from
 wireless client

[04/23/14 21:27:51.971 IST 2c 8151] 0017.7c2f.b69a Session Manager Call Client
 4975000000003e, uid 40, capwap id 7ae8c000000013,Flag 0, Audit-Session ID
 0a6987b25357e2ff00000028, method list Microsoft_NPS, policy name (null)

[04/23/14 21:27:51.971 IST 2d 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0017.7c2f.b69a, Ca3] Session start request from Client[1] for 0017.7c2f.b69a
 (method: Dot1X, method list: Microsoft_NPS, aaa id: 0x00000028), policy
[04/23/14 21:27:51.971 IST 2e 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0017.7c2f.b69a, Ca3] - client iif_id: 4975000000003E, session ID:
 0a6987b25357e2ff00000028 for 0017.7c2f.b69a


[04/23/14 21:27:51.972 IST 43 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting !EAP_RESTART on Client 0x22000025
[04/23/14 21:27:51.972 IST 44 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:enter connecting state
[04/23/14 21:27:51.972 IST 45 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025: restart connecting
[04/23/14 21:27:51.972 IST 46 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting RX_REQ on Client 0x22000025
[04/23/14 21:27:51.972 IST 47 284] ACCESS-METHOD-DOT1X-DEB:
```

```
 [0017.7c2f.b69a, Ca3] 0x22000025: authenticating state entered
[04/23/14 21:27:51.972 IST 48 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:connecting authenticating action
[04/23/14 21:27:51.972 IST 49 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting AUTH_START for 0x22000025
[04/23/14 21:27:51.972 IST 4a 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:entering request state
[04/23/14 21:27:51.972 IST 4b 291] ACCESS-METHOD-DOT1X-NOTF:
 [0017.7c2f.b69a, Ca3] Sending EAPOL packet
[04/23/14 21:27:51.972 IST 4c 291] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Platform changed src mac of EAPOL packet
[04/23/14 21:27:51.972 IST 4d 291] ACCESS-METHOD-DOT1X-NOTF:
 [0017.7c2f.b69a, Ca3] Sending out EAPOL packet
[04/23/14 21:27:51.972 IST 4e 291] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] EAPOL packet sent to client 0x22000025


[04/23/14 21:27:52.112 IST 7d 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[04/23/14 21:27:52.112 IST 7e 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:52.112 IST 7f 211] AAA SRV(00000000): Authen method=SERVER_GROUP
 Microsoft_NPS
[04/23/14 21:27:52.112 IST 80 211] AAA SRV(00000000): Selecting SG = DIAMETER
[04/23/14 21:27:52.113 IST 81 186] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Queuing an EAPOL pkt on Authenticator Q
[04/23/14 21:27:52.113 IST 82 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting EAPOL_EAP for 0x22000025
[04/23/14 21:27:52.278 IST 83 220] AAA SRV(00000000): protocol reply
 GET_CHALLENGE_RESPONSE for Authentication
[04/23/14 21:27:52.278 IST 84 220] AAA SRV(00000000): Return Authentication
 status=GET_CHALLENGE_RESPONSE
[04/23/14 21:27:52.278 IST 85 291] ACCESS-METHOD-DOT1X-DEB:[0017.7c2f.b69a,Ca3]
 Posting EAP_REQ for 0x22000025
```

Вот остаток выходных данных EAP:

```
[04/23/14 21:27:54.690 IST 12b 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:54.690 IST 12c 211] AAA SRV(00000000): Authen
 method=SERVER_GROUP Microsoft_NPS
[04/23/14 21:27:54.690 IST 12d 211] AAA SRV(00000000): Selecting SG =
 DIAMETER
[04/23/14 21:27:54.694 IST 12e 220] AAA SRV(00000000): protocol reply PASS
 for Authentication
[04/23/14 21:27:54.694 IST 12f 220] AAA SRV(00000000): Return Authentication
 status=PASS
[04/23/14 21:27:54.694 IST 130 189] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Received an EAP Success


[04/23/14 21:27:54.695 IST 186 8151] 0017.7c2f.b69a Starting key exchange with
 mobile - data forwarding is disabled
[04/23/14 21:27:54.695 IST 187 8151] 0017.7c2f.b69a 1XA: Sending EAPOL message
 to mobile, WLAN=8 AP WLAN=8
[04/23/14 21:27:54.706 IST 188 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL
 message (len 121) from mobile
[04/23/14 21:27:54.706 IST 189 8151] 0017.7c2f.b69a 1XA: Received EAPOL-Key
 from mobile
[04/23/14 21:27:54.706 IST 18a 8151] 0017.7c2f.b69a 1XK: Received EAPOL-key in
 PTK_START state (msg 2) from mobile
[04/23/14 21:27:54.706 IST 18b 8151] 0017.7c2f.b69a 1XK: Stopping retransmission
 timer
[04/23/14 21:27:54.706 IST 18c 8151] 0017.7c2f.b69a 1XA: Sending EAPOL message
 to mobile, WLAN=8 AP WLAN=8
[04/23/14 21:27:54.717 IST 18d 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL
 message (len 99) from mobile
```

```
[04/23/14 21:27:54.717 IST 18e 8151] 0017.7c2f.b69a 1XA: Received EAPOL-Key
 from mobile
[04/23/14 21:27:54.717 IST 18f 8151] 0017.7c2f.b69a 1XK: Received EAPOL-key in
 PTKINITNEGOTIATING state (msg 4) from mobile
[04/23/14 21:27:54.717 IST 190 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 1

[04/23/14 21:27:54.717 IST 191 8151] 0017.7c2f.b69a 1XK: Key exchange complete
 - updating PEM
[04/23/14 21:27:54.717 IST 192 8151] 0017.7c2f.b69a apfMs1xStateInc
[04/23/14 21:27:54.717 IST 193 8151] 0017.7c2f.b69a Change state to
 L2AUTHCOMPLETE (4) last state 8021X_REQD (3)


[04/23/14 21:27:58.277 IST 1df 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:27:58.277 IST 1e0 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:28:05.279 IST 1e1 269] DHCPD: Adding binding to hash tree
[04/23/14 21:28:05.279 IST 1e2 269] DHCPD: DHCPOFFER notify setup address
 20.20.20.5 mask 255.255.255.0


[04/23/14 21:28:05.306 IST 1f4 8151] 0017.7c2f.b69a Change state to RUN (20)
 last state DHCP_REQD (7)
```


Соответствующие дискуссии сообщества технической поддержки Cisco

Сообщество технической поддержки Cisco является форумом, в котором можно задавать вопросы и получать ответы, обмениваться предложениями и сотрудничать со своими равноправными коллегами.

См. Условные обозначения технических советов Cisco для получения информации по условным обозначениям, которые используются в данном документе.

Обновлено : 05 мая 2014
ID документа: 117684