Пример настройки защищенного доступа по протоколу Wi-Fi (WPA) в Cisco Unified Wireless Network

Содержание

Введение

Этот документ описывает, как настроить Защищенный доступ по протоколу Wi-Fi (WAP) в единой беспроводной сети Cisco (UWN).

Предварительные условия

Требования

Прежде чем выполнить данную конфигурацию, убедитесь, что вы обладаете базовыми знаниями по следующим разделам:

- WPA
- Беспроводная локальная сеть (WLAN) решения по обеспечению безопасности**Примечание:** См. Общие сведения по обеспечению безопасности беспроводной сети LAN Cisco для получения информации о решениях для безопасности беспроводных сетей Cisco.

Используемые компоненты

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

- Точка доступа облегченных серий Cisco 1000 (LAP)
- Контроллер беспроводной локальной сети (WLC) Cisco 4404, который выполняет микропрограммное обеспечение 4.2.61.0
- Клиентский адаптер Cisco 802.11a/b/g, который выполняет микропрограммное обеспечение 4.1
- Служебная программа рабочего стола Aironet (ADU), которая выполняет микропрограммное обеспечение 4.1
- Версия сервера 4.1 Cisco Secure ACS

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.

WPA и поддержка WPA2

Единая беспроводная сеть Cisco (UWN) включает поддержку WPA сертификаций Wi-Fi Alliance и WPA2. WPA был представлен Wi-Fi Alliance в 2003. WPA2 был представлен Wi-Fi Alliance в 2004. Весь Wi-Fi продуктов, Сертифицированный для WPA2, требуется, чтобы быть совместимым с продуктами, которые являются Wi-Fi, Сертифицированным для WPA.

WPA и WPA2 предлагают высокий уровень обеспечения для конечных пользователей и администраторов сети, что их данные останутся частными, и тот доступ к их сетям будет ограничен авторизованными пользователями. Оба имеют персональный и расширенные режимы операции, которые удовлетворяют отдельные потребности этих двух сегментов рынка. Расширенный режим каждого IEEE 802.1X использования и EAP для аутентификации. Персональный режим каждого Предварительного общего ключа (PSK) использования для аутентификации. Cisco не рекомендует персональный режим для бизнеса или правительственных развертываний, потому что это использует PSK для проверки подлинности пользователя. PSK не безопасен для сред предприятия.

WPA обращается ко всем известным уязвимостям WEP в исходной реализации безопасности IEEE 802.11, приносящей непосредственное решение по обеспечению безопасности WLAN и на предприятии и на средах small office office (SOHO). WPA использует TKIP для шифрования.

WPA 2 – это следующее поколение систем безопасности Wi-Fi. Это - совместимая реализация Wi-Fi Alliance ратифицированного стандарта IEEE 802.11i. Это внедряет Национальный институт стандартов и технологий (NIST), рекомендуемый использование алгоритма шифрования AES, Отвечают на Режим Протоколом Кода аутентификации сообщения Cipher Block Chaining (CCMP). WPA2 упрощает правительство FIPS

соответствие 140-2.

Сравнение WPA и типов режима WPA2

	WPA	WPA2
Расширенный режим (бизнес, правительство, образование)	• Authentication: IEEE 802.1X / EAP • Шифрование: TKIP/MIC	• Authentication: IEEE 802.1X / EAP • Шифрование: CCMP AES
Персональный режим (SOHO, Дом / персональный)	• Authentication: PSK • Шифрование: TKIP/MIC	• Authentication: PSK • Шифрование: CCMP AES

В Расширенном режиме операции и WPA и WPA2 используют 802.1X/EAP для аутентификации. 802.1X предоставляет WLAN сильным, обоюдной проверкой подлинности между клиентом и сервером проверки подлинности. Кроме того, 802.1X предоставляет динамичный для каждого пользователя, для каждого сеанса ключи шифрования, удаляя административные накладные расходы и проблемы безопасности, окружающие статические ключи шифрования.

С 802.1X учетные данные, используемые для аутентификации, такие как пароли входа, никогда не передаются в ясном, или без шифрования по беспроводной среде. В то время как типы проверки подлинности 802.1X предоставляют строгую проверку подлинности для беспроводных локальных сетей, TKIP или AES необходимы для шифрования в дополнение к 802.1X начиная со стандартного Шифрования WEP 802.11, уязвимо для сетевых атак.

Несколько типов проверки подлинности 802.1X существуют, каждый предоставляющий другой подход к аутентификации при доверии той же платформе и EAP для связи между клиентом и точкой доступа. Продукты Cisco Aironet поддерживают больше типов Аутентификации eap 802.1X, чем какие-либо другие Продукты WLAN. Поддерживаемые типы включают:

- LEAP Cisco
- ГИБКАЯ АУТЕНТИФИКАЦИЯ EAP через Безопасный, Туннелирующий (EAP-FAST)
- Transport Layer Security EAP (EAP-TLS)
- Защищенный расширяемый протокол аутентификации (PEAP)
- Туннелировавший EAP TLS (EAP-TTLS)
- EAP SUBSCRIBER IDENTITY MODULE (SIM EAP)

Другое преимущество аутентификации 802.1X является централизованным управлением для групп пользователя WLAN, включая на основе политики ключевое вращение, присвоение динамического ключа, динамическое назначение сетей VLAN и ограничение SSID. Эти функции поворачивают ключи шифрования.

В персональном режиме операции предварительный общий ключ (пароль) используется для аутентификации. В то время как Расширенный режим, как правило, требует RADIUS или другого сервера проверки подлинности в сети, персональный режим требует только точки доступа и устройства клиента.

Этот документ предоставляет примеры для настройки WPA2 (Расширенный режим) и PSK WPA2 (персональный режим) в единой беспроводной сети Cisco (UWN).

Настройка сети

В этой настройке WLC Cisco 4404 и облегченная точка доступа Cisco 1000 серии связаны через Коммутатор уровня 2. Внешний сервер RADIUS (Cisco Secure ACS) также связан с тем же коммутатором. Все устройства находятся в пределах одной подсети. Точка доступа (LAP) первоначально зарегистрирована к контроллеру. Должны быть созданы две Беспроводных локальных сети, один для Расширенного режима WPA2 и другого для персонального режима WPA2.

WLAN Расширенного режима WPA2 (SSID: Предприятие WPA2), будет использовать EAP-FAST для аутентификации Беспроводных клиентов и AES для шифрования. Сервер Cisco Secure ACS будет использоваться в качестве внешнего сервера RADIUS для аутентификации беспроводных клиентов.

WLAN Персонального режима WPA2 (SSID: PSK WPA2), будет использовать PSK WPA2 для аутентификации с предварительным общим ключом “abcdefghijk”.

Необходимо настроить устройства для этой настройки:

Настройте устройства для расширенного режима WPA2

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

Выполните эти шаги для настройки устройств для Расширенного режима WPA2 операции:

1. Конфигурация WLC для аутентификации RADIUS через внешний сервер RADIUS
2. Настройте WLAN для аутентификации расширенного режима WPA2 (EAP-FAST)
3. Настройте беспроводного клиента для расширенного режима WPA2

Конфигурация WLC для аутентификации RADIUS через внешний сервер RADIUS

Необходимо настроить WLC для переадресации на внешний сервер RADIUS учетные данные пользователя. Внешний сервер RADIUS тогда проверяет учетные данные пользователя с помощью EAP-FAST и предоставляет доступ к беспроводным клиентам.

Чтобы настроить WLC для внешнего сервера RADIUS, 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 на странице **RADIUS Authentication Servers> New**. В их числе:IP-адрес сервера RADIUSОбщий secretPort numberСостояние

сервераЭтот документ использует сервер ACS с IP-адресом 10.77.244.196.
3. **Щелкните "Применить".**

Настройте WLAN для расширенного режима WPA2 операции

Затем, настройте WLAN, который клиенты будут использовать для соединения с беспроводной сетью. SSID WLAN для расширенного режима WPA2 будет Предприятие WPA2. Данный пример назначает этот WLAN на интерфейс управления.

Выполните эти шаги для настройки WLAN и его связанных параметров:

1. **Выберите WLANs в GUI контроллера, чтобы открыть страницу WLANs.**Эта страница перечисляет WLAN, которые существуют на контроллере.
2. Нажмите **New** для создания нового WLAN.
3. Введите имя SSID WLAN и Имя профиля на странице **WLAN> New**. **Затем нажмите Apply.**Данный пример использует **Предприятие WPA2** в качестве SSID.
4. **После создания новой WLAN появляется страница WLAN > Edit для новой WLAN.** На этой странице можно определить различные параметры, определенные для этого WLAN. Это включает Общую политику, Политику безопасности, политики QoS и Усовершенствованные параметры.
5. В соответствии с Общей политикой, установите флажок **Проверки состояния** для включения WLAN.
6. Если вы хотите, чтобы AP передал SSID в своих кадрах неисправность, проверьте флажок **Broadcast SSID**.
7. **Щелкните вкладку Безопасность.** Под безопасностью уровня 2 выберите **WPA+WPA2**.Это включает аутентификацию WPA для WLAN.
8. Прокрутите страницу вниз для изменения **Параметров WPA+WPA2**.В данном примере выбраны Политика WPA2 и шифрование AES.
9. Под Подлинным Ключевым Mgmt выберите **802.1x**.Это включает WPA2 с помощью 802.1X/АУТЕНТИФИКАЦИИ EAP и шифрования AES для WLAN.
10. Нажмите вкладку **AAA Servers**. Под Серверами проверки подлинности выберите соответствующий IP-адрес сервера.В данном примере, 10.77.244.196 используется в качестве сервера RADIUS.
11. **Щелкните "Применить".Примечание:** Это - единственный EAP, устанавливающий, который должен быть настроен на контроллере для Аутентификации eap. Все другие конфигурации, определенные для EAP-FAST, должны быть реализованы на сервере RADIUS и клиентах, которые должны аутентифицироваться.

Настройте сервер RADIUS для аутентификации расширенного режима WPA2 (EAP-FAST)

В данном примере Cisco Secure ACS используется в качестве внешнего сервера RADIUS. Выполните эти шаги для настройки сервера RADIUS для аутентификации EAP-FAST:

1. Создайте базу данных пользователей для аутентификации клиентов
2. Добавьте WLC как клиента AAA к серверу RADIUS
3. Настройте аутентификацию EAP-FAST на сервере RADIUS с анонимной внутриполосной инициализацией PAC**Примечание:** EAP-FAST может быть настроен

или с Анонимной Внутриполосной Инициализацией PAC или с Аутентифицируемой Внутриполосной Инициализацией PAC. Данный пример использует Анонимную Внутриполосную Инициализацию PAC. Для получения дальнейшей информации и примеры при настройке FAST EAP с Анонимной Внутриполосной Инициализацией PAC и Аутентифицируемой Внутриполосной Инициализацией, обратитесь к Аутентификации EAP-FAST с Примером конфигурации Внешнего сервера RADIUS и Контроллерами беспроводной локальной сети.

Создайте базу данных пользователей для аутентификации клиентов EAP-FAST

Выполните эти шаги для создания базы данных пользователей для клиентов EAP-FAST на ACS. Данный пример настраивает имя пользователя и пароль клиента EAP-FAST как User1 и User1, соответственно.

1. От GUI ACS в панели навигации выберите **User Setup**. Создайте радио нового пользователя, и затем нажмите **Add/Edit**, чтобы перейти к странице Edit этого пользователя.
2. От страницы Edit Настройки пользователя настройте Настоящее имя и Описание, а также Вводы пароля как показано в данном примере.Этот документ использует **Внутреннюю базу данных ACS** для Проверки подлинности с помощью пароля.
3. Выберите **ACS Internal Database** из раскрывающегося окна Проверки подлинности с помощью пароля.
4. Настройте все другие необходимые параметры и нажмите **Submit**.

Добавьте WLC как клиента AAA к серверу RADIUS

Выполните эти шаги для определения контроллера как клиент AAA на сервере ACS:

1. **В ACS GUI нажмите Network Configuration.** Под Добавить разделом клиента AAA страницы Network Configuration **нажмите Add Запись** для добавления WLC как клиент AAA к серверу RADIUS.
2. От страницы AAA Client определите название WLC, IP-адреса, общего секретного ключа и метода аутентификации (Airespace RADIUS/Cisco). Сведения о серверах аутентификации, отличной от ACS, см. в документации от производителя.**Примечание:** Общий секретный ключ на WLC и сервере ACS должны совпадать. При вводе общего секретного ключа необходимо учитывать регистр.
3. **Нажмите кнопку Submit+Apply (Отправить и применить).**

Настройте аутентификацию EAP-FAST на сервере RADIUS с анонимной внутриполосной инициализацией PAC

Анонимная внутриполосная инициализация

Это - один из двух внутриполосных методов инициализации, в которых ACS устанавливает защищенное соединение с клиентом конечного пользователя в целях предоставления клиенту с новым PAC. Эта опция позволяет анонимное подтверждение связи TLS между клиентом конечного пользователя и ACS.

Этот метод управляет в Аутентифицируемом Протоколе соглашения Диффи-Хеллмэнки (ADHP) туннелем, прежде чем узел будет аутентифицировать сервер ACS.

Затем ACS требует аутентификации EAP-MS-CHAPv2 пользователя. При успешной аутентификации пользователя ACS устанавливает туннель Диффи-Хеллмана с клиентом конечного пользователя. ACS генерирует PAC для пользователя и передает ему конечному пользователю клиента в этом туннеле, наряду с информацией об этом ACS. Этот метод инициализации EAP-MSCHAPv2 использования как метод аутентификации в фазовом нуле и EAP-GTC в фазе два.

Поскольку не прошедший поверку подлинности сервер настроен, не возможно использовать незашифрованный пароль. Поэтому только учетные данные MS-CHAP могут использоваться в туннеле. MSCHAPv2 используется, чтобы удостоверить личность узла и получить PAC для дальнейших сеансов аутентификации (MS-CHAP EAP будет использоваться только в качестве внутреннего метода).

Выполните эти шаги для настройки аутентификации EAP-FAST в сервере RADIUS для анонимной внутриполосной инициализации:

1. Нажмите **System Configuration** от GUI сервера RADIUS. От страницы System Configuration выберите **Global Authentication Setup**.
2. От страницы настройки Глобальной аутентификации нажмите **EAP-FAST Configuration**, чтобы перейти к странице настроек EAP-FAST.
3. От Страницы настроек EAP-FAST проверьте флажок **Allow EAP-FAST** для включения EAP-FAST в сервере RADIUS.
4. Настройте Активный/Исключенный TTL главного ключа (Время существования) значения, как желаемый или установите его в значение по умолчанию как показано в данном примере.См. Главные ключи для получения информации об Активных и Исключенных главных ключах. Кроме того, обратитесь к Главным ключам и TTL PAC для получения дополнительной информации.Поле Authority ID Info представляет текстовую идентичность этого сервера ACS, который конечный пользователь может использовать для определения который сервер ACS аутентифицироваться против. Заполнение этого поля является обязательным.Клиентская начальная буква отображается, поле сообщения задает сообщение, которое будет передаваться пользователям, которые аутентифицируются с клиентом EAP-FAST. Максимальная длина составляет 40 символов. Пользователь будет видеть начальное сообщение только если поддержки клиентов конечного пользователя показ.
5. Если вы хотите, чтобы ACS выполнил анонимную внутриполосную инициализацию PAC, проверьте **Позволение анонимного внутриполосного** флажка **инициализации PAC**.
6. **Позволенные внутренние методы** — Эта опция определяет, какие внутренние методы EAP могут работать в туннеле TLS EAP-FAST. Для анонимной внутриполосной инициализации необходимо включить EAP-GTC и MS-CHAP EAP для обратной совместимости. При выборе Allow анонимная внутриполосная инициализация PAC необходимо выбрать EAP-MS-CHAP (фазовый нуль) и EAP-GTC (фаза два).

Настройте беспроводного клиента для расширенного режима WPA2 операции

Следующий шаг должен настроить беспроводного клиента для Расширенного режима WPA2 операции.

Выполните эти шаги для настройки беспроводного клиента для Расширенного режима WPA2.

1. Из окна Aironet Desktop Utility нажмите **Profile Management> New** для создания профиля для пользователя WLAN Предприятия WPA2.Как отмечалось ранее, этот документ использует название WLAN/SSID в качестве **Предприятия WPA2** для беспроводного клиента.
2. От Окна управления Профиля нажмите **Вкладку Общие** и настройте Имя профиля, Имя клиента и название SSID как показано в данном примере. **Затем нажмите кнопку ОК**
3. Нажмите **Вкладку Безопасность** и выберите **WPA/WPA2/CCKM** для включения режима работы WPA2. Под Типом EAP WPA/WPA2/CCKM выберите **EAP-FAST**. Нажмите **Configure** для настройки значения EAP-FAST.
4. Из окна Configure EAP-FAST проверьте флажок **Allow Automatic PAC Provisioning**. Если вы захотите настроить анонимную инициализацию PAC, то MS-CHAP EAP будет использоваться в качестве единственного внутреннего метода в фазовом нуле.
5. Выберите MSCHAPv2 User Name and Password в качестве метода аутентификации от раскрывающегося окна Метода аутентификации EAP-FAST. **Нажмите кнопку Configure (Настроить).**
6. Из окна Configure MSCHAPv2 User Name and Password выберите соответствующие параметры настройки имени пользователя и пароля.Данный пример выбирает **Automatically Prompt for User Name and Password**.То же имя пользователя и пароль должны быть зарегистрированы в ACS. Как отмечалось ранее, данный пример использует User1 и User1 соответственно как имя пользователя и пароль. Кроме того, обратите внимание, что это - анонимная внутриполосная инициализация. Поэтому клиент не может проверить серверный сертификат. Необходимо удостовериться, что снят Проверить флажок Установления личности Сервера.
7. **Нажмите кнопку ОК.**

Проверьте расширенный режим WPA2 операции

Выполните эти шаги, чтобы проверить, работает ли ваша конфигурация Расширенного режима WPA2 должным образом:

1. Из окна Aironet Desktop Utility выберите **Предприятие WPA2** профиля и нажмите **Activate** для активации профиля беспроводного клиента.
2. Если вы включили MS-CHAP ver2 как свою аутентификацию, то клиент вызовет для имени пользователя и пароля.
3. Во время обработки EAP-FAST пользователя вам предложит клиент запросить PAC от сервера RADIUS. Когда вы **нажимаете кнопку Да**, инициализация PAC запускается.
4. После успешной инициализации PAC в фазовом нуле придерживается фаза 1 и два, и процедура успешной аутентификации имеет место.После успешной аутентификации беспроводной клиент привязан к Предприятию WPA2 WLAN. Вот снимок экрана:Можно также проверить, получает ли сервер RADIUS и проверяет запрос аутентификации от беспроводного клиента. Чтобы выполнить данное действие, проверьте отчеты Passed Authentications и Failed Attempts на сервере ACS. Данные отчеты доступны в Reports и Activities на сервере.

Настройте устройства для персонального режима WPA2

Выполните эти шаги для настройки устройств для Персонального режима WPA2 операции:

1. Настройте WLAN для аутентификации персонального режима WPA2
2. Настройте беспроводного клиента для персонального режима WPA2

Настройте WLAN для персонального режима WPA2 операции

Необходимо настроить WLAN, который клиенты будут использовать для соединения с беспроводной сетью. SSID WLAN для персонального режима WPA2 будет Персональным WPA2. Данный пример назначает этот WLAN на интерфейс управления.

Выполните эти шаги для настройки WLAN и его связанных параметров:

1. **Выберите WLANs в GUI контроллера, чтобы открыть страницу WLANs.**Эта страница перечисляет WLAN, которые существуют на контроллере.
2. Нажмите **New** для создания нового WLAN.
3. Введите имя SSID WLAN, Имя профиля и ИДЕНТИФИКАТОР WLAN на странице WLAN> New. **Затем нажмите Apply.**Использование данного примера**, Персональное WPA2** как SSID.
4. **После создания новой WLAN появляется страница WLAN > Edit для новой WLAN.** На этой странице можно определить различные параметры, определенные для этого WLAN. Это включает Общую политику, Политику безопасности, политики QoS и Усовершенствованные параметры.
5. В соответствии с Общей политикой, установите флажок **Проверки состояния** для включения WLAN.
6. Если вы хотите, чтобы AP передал SSID в своих кадрах неисправность, проверьте флажок **Broadcast SSID**.
7. **Щелкните вкладку Безопасность.** Под Безопасностью Уровня выберите **WPA+WPA2**.Это включает аутентификацию WPA для WLAN.
8. Прокрутите страницу вниз для изменения **Параметров WPA+WPA2**.В данном примере выбраны Политика WPA2 и шифрование AES.
9. Под Подлинным Ключевым Mgmt выберите **PSK** для включения PSK WPA2.
10. Введите предварительный общий ключ в соответствующее поле как показано.**Примечание:** Предварительный общий ключ, используемый на WLC, должен совпасть с тем, настроенным на беспроводных клиентах.
11. **Щелкните "Применить".**

Настройте беспроводного клиента для персонального режима WPA2

Следующий шаг должен настроить беспроводного клиента для Персонального режима WPA2 операции.

Выполните эти шаги для настройки беспроводного клиента для Персонального режима WPA2:

1. Из окна Aironet Desktop Utility нажмите **Profile Management> New** для создания профиля для пользователя WLAN PSK WPA2.
2. От Окна управления Профиля нажмите **Вкладку Общие** и настройте Имя профиля, Имя клиента и название SSID как показано в данном примере. **Затем нажмите кнопку OK.**

3. Нажмите **Вкладку Безопасность** и выберите **WPA/WPA2 Passphrase** для включения режима работы PSK WPA2. Нажмите **Configure** для настройки предварительного общего ключа WPA-PSK.
4. Введите общий ключ и нажмите **OK**.

Проверьте персональный режим WPA2 операции

Выполните эти шаги, чтобы проверить, работает ли ваша конфигурация Расширенного режима WPA2 должным образом:

1. Из окна Aironet Desktop Utility выберите **Персональный WPA2** профиль и нажмите **Activate** для активации профиля беспроводного клиента.
2. Как только профиль активирован, беспроводной клиент связывается к WLAN после успешной аутентификации.Вот снимок экрана:

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Эти **команды отладки** будут полезны для устранения проблем конфигурации:

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **debug dot1x events enable** — Включает отладку всех событий dot1x. Вот выходные данные отладки в качестве примера на основе успешной аутентификации:**Примечание:** Некоторые линии от этих выходных данных были перемещены во вторые линии из-за ограничений длины.(Cisco Controller)>**debug dot1x events enable** Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 **Received EAPOL START from mobile 00:40:96:af:3e:93** Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 **Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2)** Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 **Received Identity Response (count=2) from mobile 00:40:96:af:3e:93** Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 **Processing Access-Challenge for mobile 00:40:96:af:3e:93**
.....
.....
.....
..... Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43)** Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Processing Access-Challenge for mobile 00:40:96:af:3e:93** Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)** Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)** Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 19 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007:

00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 26) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for mobile00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to mobile 00:4096:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ===> 20 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 24 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access-Challenge for mobile 00:40:96:af:3e:93** Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25)** Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)** Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access-Accept for mobile**

00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Creating a new PMK Cache Entry for tation 00:40:96:af:3e:93 (RSN 0)** Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending EAP-Success to mobile 00:40:96:af:3e:93 (EAP Id 25)** Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending default RC4 key to mobile 00:40:96:af:3e:93** Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending Key-Mapping RC4 key to mobile 00:40:96:af:3e:93** Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Received Auth Success while in Authenticating state for mobile 00:40:96:af:3e:93**

- **пакет debug dot1x включает** — Включает отладку пакетных сообщений 802.1x.
- **debug aaa events enable** — Включает выходные данные отладки всех событий aaa.

Дополнительные сведения

- WPA2 - защищенный доступ по протоколу Wi-Fi 2
- Пример конфигурации проверки подлинности EAP-FAST с контроллерами беспроводной сети и внешним сервером RADIUS
- Пример конфигурации аутентификации EAP в контроллерах WLAN (WLC)
- Обзор конфигурации WPA
- Поддержка беспроводного продукта
- Cisco Systems – техническая поддержка и документация