Internet Engineering Task Force (IETF)
Request for Comments: 7652
Updates: 6887
Category: Standards Track
ISSN: 2070-1721

M. Cullen
S. Hartman
Painless Security
D. Zhang
T. Reddy
Cisco

September 2015

Механизм аутентификации PCP

Port Control Protocol (PCP) Authentication Mechanism

Тезисы

Хост IPv4 или IPv6 может использовать протокол PCP[1] для гибкого управления информацией об отображениях адресов и портов на трансляторах NAT[2] или межсетевых экранах для коммуникаций с удаленными хостами. Однако неконтролируемое создание или удаление отображений адресов IP в таких сетевых устройствах может вызывать проблемы безопасности и его следует избегать. В некоторых случаях от клиентов может требоваться подтверждение его полномочий на изменение, создание или удаление отображений PCP. В данном документе описывается реализуемый в основной полосе (in-band) механизм аутентификации для PCP, который может применяться в таких случаях. Для аутентификации между устройствами PCP используется расширяемый протокол аутентификации (EAP[3]).

Данный документ служит обновлением RFC 6887.

Статус документа

Этот документ относится к категории проектов стандартов (Internet Standards Track).

Документ является результатом работы IETF[4] и представляет собой согласованное мнение сообщества IETF. Документ был вынесен на публичное рассмотрение и одобрен для публикации IESG[5]. Дополнительная информация о документах BCP представлена в разделе 2 документа RFC 5741.

Информация о текущем статусе этого документа, обнаруженных ошибках и способах обратной связи может быть найдена по ссылке http://www.rfc-editor.org/info/rfc7652.

Оглавление

[1]Port Control Protocol — протокол управления портом.
[2]Network Address Translator — транслятор сетевых адресов.
[3]Extensible Authentication Protocol — расширяемый протокол аутентификации.
[4]Internet Engineering Task Force.
[5]Internet Engineering Steering Group.

1 Введение

Используя PCP [RFC6887], приложение может гибко управлять информацией об отображениях адресов IP на своих трансляторах сетевых адресов (NAT) и межсетевых экранах (МСЭ), а также контролировать правила обработки входящих и исходящих пакетов IP. Поскольку устройства NAT и МСЭ играют важную роль в архитектуре сетевой безопасности, возникает множество ситуаций, в которых требуется аутентификация и контроль доступа для предотвращения несанкционированного доступа в таким устройствам. В этом документе определено защитное расширение PCP, которое позволяет серверам PCP аутентифицировать своих клиентов с помощью расширяемого протокола аутентификации (EAP). Сообщения EAP инкапсулируются в сообщения PCP.

В документе рассмотрены вопросы устройства данного расширения, включая:

- потерю сообщений EAP в процессе передачи;
- нарушение порядка доставки сообщений EAP;
- генерацию транспортных ключей;
- защиту целостности и аутентификацию источника данных для сообщений PCP;
- скорость алгоритма.

Описанный в этом документе механизм соответствует требованиям безопасности для расширенной модели угроз (Advanced Threat Model), описанной в базовой спецификации PCP [RFC6887]. Этот механизм может использоваться для защиты PCP в следующих ситуациях:

- на оборудовании защиты (например, корпоративных МСЭ), которое не создает неявных отображений для конкретного трафика;
- на оборудовании (например, CGN[1] или МСЭ сервис-провайдера), обслуживающем множество административных доменов и не имеющем механизмов безопасной изоляции трафика разных доменов;
- для любых реализаций, которые хотят достаточно мягко разрешать организацию отображений для входящих соединений с машинами, расположенными за устройствами NAT или МСЭ.

2 Терминология

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с RFC 2119 [RFC2119].

Большая часть используемых в документе терминов определена в [RFC6887].

PCP client — клиент PCP

Программный экземпляр PCP, отвечающий за подачу PCP-запросов серверу PCP. В данном документе клиентом PCP считается также партнер EAP [RFC3748] и ответственность за предоставление свидетельств при аутентификации ложится на клиента PCP.

PCP server — сервер PCP

[1] Carrier-Grade NAT - NAT операторского уровня.

Программный экземпляр PCP, размещенный на управляемом PCP устройстве, который принимает запросы PCP от клиентов PCP и организует в ответ соответствующие состояния. В этом документе сервер PCP объединен с аутентификатором EAP [RFC3748]. Следовательно, при необходимости сервер PCP может проверить свидетельства, представленные клиентом PCP и принять решение о предоставлении клиента доступа по результатам такой проверки.

PCP-Authentication (PA) session — сеанс аутентификации PCP

Последовательность сообщений PCP, передаваемых между клиентом и сервером. Сообщения PCP, относящиеся к данной сессии, включают сообщения PA, используемые для аутентификации EAP, распространения ключей и управления сессией, а также обычные сообщения PCP, защищенные с помощью ключей, распространенных в процессе аутентификации. Каждой сессии PA присваивается свой идентификатор (Session ID).

Session partner — партнер по сессии

Реализация PCP, вовлеченная в сеанс PA. Каждая сессия PA включает двух партнеров (клиент и сервер PCP).

PCP device — устройство PCP

Клиент или сервер PCP.

Session lifetime — время жизни сессии

Время жизни, связанное с сеансом PA. Время жизни сессии PA определяет срок действия полномочий, предоставленных клиенту PCP.

PA Security Association (PCP SA) — защищенная связь PCP

Связь, организуемая между клиентом и сервером PCP, путем использования общего ключевого материала и связанного контекста. Сформированная связь служит для защиты двухстороннего сигнального трафика PCP между клиентом и сервером PCP.

Master Session Key (MSK) — первичный сеансовый ключ

Ключ, созданный партнерами по сессии PA с использованием метода генерации EAP (например, [RFC5448]).

PCP-Authentication (PA) message — аутентификационное сообщение

Сообщение PCP, содержащее код операции AUTHENTICATION. Сообщение PA, отправленное сервером PCP клиенту PCP будем называть далее сообщением PA-Server, а сообщение PA от клиента к серверу PCP — сообщением PA-Client. Таким образом, сообщения PA-Server представляют собой отклики PCP [RFC6887], а сообщения PA-Client — запросы PCP. В данном документе (параграф 5.5) определена опция PA_AUTHENTICATION_TAG, служащая для защиты целостности и аутентификации источника сообщений PA.

Common PCP message — обычное сообщение PCP

Сообщение PCP, не содержащее кода операции AUTHENTICATION. В этом документе определена опция AUTHENTICATION_TAG, служащая для защиты целостности и аутентификации источника обычных сообщений PCP.

3 Детали протокола

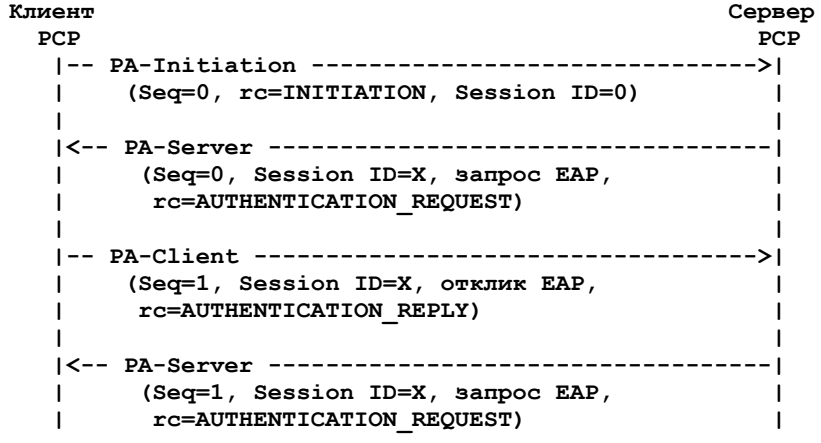
3.1 Инициирование сессии

В начале сессии PA клиент и сервер PCP должны обменяться серией сообщений PA для выполнения аутентификации EAP. Каждое сообщение PA **должно** содержать код операции AUTHENTICATION и может включать опции для решения тех или иных задач (например, доставка аутентификационных сообщений и управление сессией). Специфические для операции AUTHENTICATION данные включают два поля: Session ID и Sequence Number. Поле Session ID служит для идентификации сессии PA, к которой относится сообщение. Поле Sequence Number применяется для детектирования нарушений порядка доставки и дубликатов сообщений.

3.1.1 Аутентификация по инициативе клиента

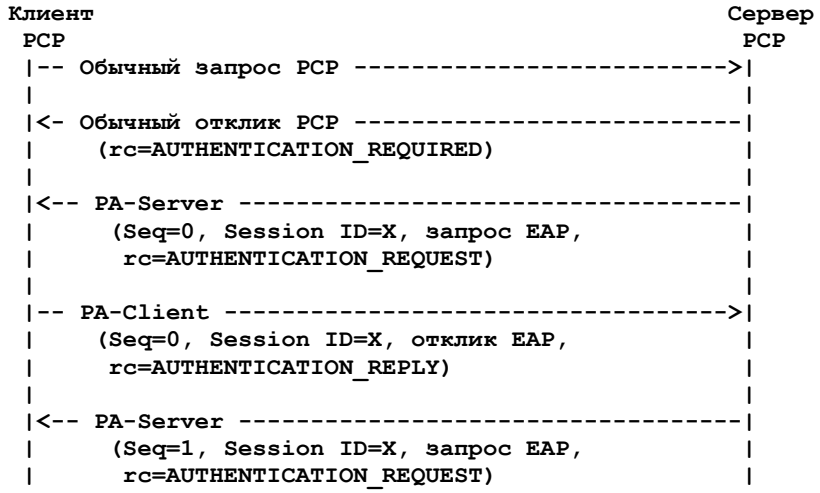
Когда клиент PCP намерен заранее инициировать сессию PA с сервером PCP, он передает сообщение PA-Initiation (сообщение PA-Client с кодом результата INITIATION) серверу PCP. В параграфе 5.1 описано изменение формата запросов PCP с учетом кодов результата, используемых механизмом аутентификации PCP. В зависящих от кода операции данных такого сообщения поля Session ID и Sequence Number устанавливаются в 0. Сообщение PA-Client **должно** также включать опцию NONCE (определена в параграфе 5.3) со случайным значением.

После получения PA-Initiation сервер PCP, если он согласен инициировать сессию PA с клиентом PCP, будет отвечать сообщением PA-Server, которое содержит запрос EAP и код результата AUTHENTICATION_REQUEST. В дополнение к этому сервер **должен** выделить уникальный идентификатор сессии и поместить его в поле Session ID зависящих от операции данных сообщения PA-Server. В поле Sequence Number устанавливается значение 0. Сообщение PA-Server **должно** включать опцию NONCE, в которой клиенту возвращается принятое от него одноразовое значение. Это значение используется клиентом для проверки «свежести» полученного сообщения. В последующие сообщения данной сессии PA **должен** включаться идентификатор сессии.



3.1.2 Аутентификация по инициативе сервера

В ситуации, когда сервер PCP получает обычный запрос PCP от клиента, для которого требуется аутентификация, сервер отвергает такой запрос с кодом ошибки AUTHENTICATION_REQUIRED и может отправить незапрошенное сообщение PA-Server для организации сессии PA. Поле Result Code в таком сообщении PA-Server содержит значение AUTHENTICATION_REQUEST. Кроме того, сервер **должен** выделить для сессии идентификатор (Session ID) и передать его в сообщении PA-Server. Для поля Sequence Number в сообщении PA-Server устанавливается нулевое значение. Если клиент повторит обычный запрос PCP до завершения аутентификации EAP, он получит от сервера отклик с кодом ошибки AUTHENTICATION_REQUIRED. В последующих сообщениях PA данной сессии поле Session ID будет помогать партнерам идентифицировать относящиеся к сессии сообщения. При получении клиентом PCP начального сообщения PA-Server от сервера PCP он может ответить сообщением PA-Client или отбросить запрос без уведомления сервера в соответствии со своей локальной политикой. К сообщению PA-Client **может** быть добавлена опция NONCE с одноразовым случайным значением. В этом случае сервер в следующем сообщении PA-Server **должен** вернуть полученное одноразовое значение в опции NONCE.



3.1.3 Аутентификация с применением EAP

В сессии PA запрос EAP передается в сообщении PA-Server, а отклик EAP — в сообщении PA-Client. EAP полагается на услуги нижележащего протокола в плане обеспечения гарантий доставки, нарушение порядка и потерю пакетов в процессе передачи нужно детектировать и исправлять. Следовательно, после отправки сообщения PA-Server сервер PCP не будет передавать в данной сессии PA новых сообщений PA-Server до получения отклика PA-Client с корректным порядковым номером (и наоборот). Если клиент PCP получает сообщение PA с запросом EAP и по той или иной причине не может сразу же создать отклик EAP (например, ждет вмешательства оператора для получения данных, требуемых сообщению EAP, или дополнительных сообщений PA для сборки сообщения EAP из фрагментов), устройство PCP **должно** ответить сообщением PA-Acknowledgement (сообщение PA с опцией RECEIVED_PAK) для индикации получения запроса. Это не только позволяет избежать ненужных повторов сообщений PA, но и обеспечивает надежную доставку в тех случаях, когда устройству PCP требуется собрать множество сообщений PA с фрагментами запроса EAP для генерации отклика EAP. Число сообщений EAP в обмене между клиентом и сервером PCP зависит от используемого EAP метода аутентификации.

В этой модели клиент и сервер PCP **должны** применять для аутентификации метод EAP с генерацией ключей. В частности, реализации PCP с аутентификацией **должны** поддерживать EAP-TTLS[1] [RFC5281] и **следует** также поддерживать TEAP[2] [RFC7170]. Следовательно, после успешного завершения процедуры аутентификации будет генерироваться первичный сеансовый ключ MSK. Если клиент и сервер PCP хотят генерировать транспортный ключ с использованием MSK, они должны согласовать псевдо-случайную функцию (PRF[3]) для создания транспортного ключа и алгоритм MAC[4] для аутентификации источника последующих сообщений PCP. Для решения этой задачи сервер должен добавить набор опций PRF и MAC_ALGORITHM в конец исходного сообщения PA-Server. Каждая опция PRF включает поддерживаемую сервером PRF, а каждая опция MAC_ALGORITHM — поддерживаемый алгоритм MAC. Кроме того, к первому сообщению PA-Server сервер **может** добавить опцию ID_INDICATOR (см. параграф 5.11), помогающую клиенту выбрать свидетельства (credential). После получения опций клиент PCP **должен** выбрать PRF и алгоритм MAC, которые он хочет использовать, и добавить соответствующие опции PRF и MAC_ALGORITHM в следующее сообщение PA-Client.

После аутентификации EAP сервер PCP передает сообщение PA-Server для индикации результатов аутентификации EAP и проверки полномочий PCP. При успешной аутентификации EAP в сообщении PA-Server указывается код результата AUTHENTICATION_SUCCEEDED. В этом случае перед отправкой сообщения PA-Server сервер PCP **должен** обновить PCP SA с указанием MSK и транспортного ключа, а также использовать созданный транспортный ключ для генерации подписи к сообщению. Подпись передается в опции PA_AUTHENTICATION_TAG для PCP Auth. Более подробное описание генерации аутентификационных данных приведено в параграфе 6.1. Кроме того, сообщение PA-Server **должно** также включать опцию SESSION_LIFETIME (см. параграф 5.9), указывающее срок существования сессии PA (т. е., время жизни MSK). После приема сообщения PA-Server клиенту PCP нужно создать ответное сообщение PA-Client. Если клиент PCP тоже аутентифицировал сервер PCP, в качестве кода результата в сообщении PA-Client указывается AUTHENTICATION_SUCCEEDED. Кроме того, клиенту PCP нужно обновить PCP SA, включив ключ MSK и транспортный ключ и использовать полученный транспортный ключ для защиты сообщения. С этого момента все сообщения PCP в данной сессии будут защищаться с использованием транспортного ключа и алгоритма MAC, указанного в PCP SA. Первое защищенное сообщение PA-Client от клиента **должно** включать набор

[1]Extensible Authentication Protocol Tunneled Transport Layer Security.
[2]Tunnel Extensible Authentication Protocol.
[3]Pseudorandom Function.
[4]Message Authentication Code — код аутентификации сообщения.

опций PRF и MAC_ALGORITHM, полученных от сервера PCP. Сервер PCP проверяет соответствие полученного набоа алгоритмов отправленному им для обнаружения атак на снижение уровня защиты. При обнаружении такой атаки сервер **должен** передать сообщение PA-Server с кодом результата DOWNGRADE_ATTACK_DETECTED и прервать сессию. Если клиент PCP передает обычный запрос PCP в сессии PA без опции AUTHENTICATION_TAG, сервер PCP отвергает такой запрос, возвращая код ошибки AUTHENTICATION_REQUIRED.

Если клиент/сервер PCP не может аутентифицировать партнера по сессии, устройство передает сообщение PA с кодом результата AUTHENTICATION_FAILED. Если аутентификация EAP завершилась успешно, а проверка полномочий - отказом, принимающее решение устройство передает сообщение PA с кодом результата AUTHORIZATION_FAILED. В этих двух случаях после передачи сообщения PA сессия PA **должна** быть разорвана незамедлительно. Независимые клиенты PCP на хосте могут создавать множество сессий PA с сервером PCP.

3.2 Восстановление потерянной сессии PA

Если сервер PCP сбросил или потерял PCP SA в результате перезапуска, сбоя питания или по иной причине, он передает клиенту PCP незапрошенный отклик ANNOUNCE, как описано в параграфе 14.1.3 [RFC6887]. При получении отклика ANNOUNCE с аномальным значением Epoch Time клиент PCP понимает, что сервер мог потерять состояние. Отклик ANNOUNCE может оказаться поддельным (атака), легитимным или не замеченным клиентом. Эти три случая описаны ниже.

- Клиент PCP передает защищенный (целостность) запрос ANNOUNCE по индивидуальному адресу сервера PCP для того, чтобы определить получен отклик ANNOUNCE от потерявшего состояние сервера PCP или является частью атаки.
    - Если от сервера PCP приходит отклик об успешном завершении с защитой целостности, клиент PCP считает, что у сервера PCP нет потерянной сессии PA, а незапрошенный отклик ANNOUNCE передан атакующим.
    - Если сервер PCP отвечает на запрос ANNOUNCE кодом ошибки UNKNOWN_SESSION_ID, клиент PCP **должен** инициировать полную аутентификацию EAP с этим сервером PCP, как описано в параграфе 3.1.1. После успешной аутентификации EAP клиент PCP обновляет PCP SA и передает новые запросы PCP общего назначения для восстановления утраченного отображения.
- В случае, когда сервер PCP потерял PCP SA, но не информировал об этом клиента PCP, а клиент PCP передал запрос PCP с защитой целостности, сервер PCP отвергает такой запрос с кодом ошибки UNKNOWN_SESSION_ID. Клиент PCP в этом случае инициирует полную аутентификацию EAP с сервером PCP (см. параграф 3.1.1) и после ее успешного завершения обновляет PCP SA.

Если клиент PCP сбрасывает или теряет PCP SA в результате перезагрузки, сбоя питания или по иной причине и передает обычный запрос PCP, сервер PCP отвергает такой запрос с кодом ошибки AUTHENTICATION_REQUIRED. Клиент PCP **должен** выполнить аутентификацию с помощью опции AUTHENTICATION_TAG. Сервер PCP **должен** обновить PCP SA после успешной аутентификации EAP.

3.3 Прерывание сессии

Сессия PA может быть явно прервана любым из ее участников. Сервер PCP может явно запросить разрыв сессии, передав незапрошенный отклик PA, указывающий разрыв (отклик PA с кодом результата SESSION_TERMINATED). При получении такого сообщения клиент PCP **должен** ответить сообщением PA с индикацией разрыва сессии и затем удалить соответствующую PCP SA. С учетом возможной потери пакетов сервер PCP **может** передавать отклик PA о разрыве сессии до 10 раз (с корректировкой значения Epoch Time в каждом сообщении с учетом прошедшего времени), при этом (1) интервал между первым и вторым сообщениями должен быть не менее 250 мсек и (2) при каждом следующем повторе интервал должен увеличиваться по не менее, чем вдвое.

Клиент PCP может явно разорвать сессию путем передачи запроса PA, указывающего разрыв (запрос PA с кодом результата SESSION_TERMINATED). После получения от клиента PCP такого сообщения сервер PCP **должен** ответить сообщением PA о разрыве сессии и незамедлительно удалить PCP SA. Когда клиент PCP получает отклик PA о разрыве сессии, он **должен** незамедлительно удалить соответствующую PCP SA.

3.4 Повторная аутентификация сессии

Партнер по сессии может принять решение о повторной аутентификации EAP, если ему нужно обновить PCP SA без инициирования новой сессии PA. Например, повторная аутентификация может возникать в случаях:

- необходимость продления срока действия сессии;
- достижение максимального значения порядковых номеров (в частности, когда порядковый номер достигает значения $2^{32} - 2^{16}$, партнер **должен** повторить аутентификацию).

Если сервер PCP хочет инициировать повторную аутентификацию, он отправляет клиенту PCP сообщение PA-Server с кодом результата RE-AUTHENTICATION, показывающим желание повторной аутентификации. Если клиент считает возможным повтор аутентификации, он передает серверу PCP сообщение PA-Client с кодом результата RE-AUTHENTICATION. После этого партнеры обмениваются сообщениями PA для передачи используемых при повторной аутентификации сообщений EAP. В процессе повторной аутентификации партнеры защищают целостность своих сообщений PA с использованием ключа и алгоритма MAC из текущей PCP SA, Порядковые номера, связанные с этими сообщениями, будут возрастать, как описано в параграфе 6.4. В сообщении PA-Server с запросом EAP указывается код результата AUTHENTICATION_REQUIRED, а в сообщении PA-Client с откликом EAP - AUTHENTICATION_REPLY.

При успешном завершении повторной аутентификации EAP в последнем сообщении PA-Server указывается код результата AUTHENTICATION_SUCCEEDED. В этом случае перед отправкой сообщения PA-Server сервер PCP **должен** обновить SA и использовать новый ключ для генерации подписи сообщения PA-Server и последующих сообщений PCP. Кроме того, в конце сообщения PA-Server **должна** добавляться опция SESSION_LIFETIME, показывающая срок действия новой сессии PA. Порядковые номера сообщений PA и PCP должны быть сброшены в 0.

При отказе аутентификации EAP в поле результата последнего сообщения PA-Server указывается код AUTHENTICATION_FAILED. Если аутентификация EAP прошла, но проверка полномочий завершилась отказом, в последнем сообщении PA-Server указывается код ошибки AUTHORIZATION_FAILED. В обоих случаях сессия PA должна разрываться сразу же после завершения последнего обмена сообщениями PA. Если по тем или иным причинам повторная аутентификация не была выполнена и срок действия сессии истек, сессия PA **должна** быть разорвана без промедления.

В процессе выполнения повторной аутентификации партнеры могут обмениваться в сессии и обычными сообщениями PCP. Такие сообщения **должны** защищаться с использованием текущей SA, пока не будет создана новая SA. Последовательность обмена сообщениями EAP для повторной аутентификации не меняется в зависимости от инициатора. Если сервер PCP получает запрос повторной аутентификации от клиента PCP после того, как сам сервер отправил подобный запрос, ему следует отбросить свой запрос и ответить на клиентский запрос.

4 Защищенная связь PA

В начале сессии PA каждое устройство PCP должно создать и инициализировать информацию о состоянии для новой защищенной связи PA (PCP SA) с целью поддержки данных о состоянии в течение срока действия сессии PA. Параметры сессии PCP SA включают:

- IP-адрес и номер порта UDP клиента PCP.
- IP-адрес и номер порта UDP сервера PCP.
- Идентификатор сессии.
- Порядковый номер для следующего исходящего сообщения PA.
- Порядковый номер для следующего входящего сообщения PA.
- Порядковый номер для следующего исходящего сообщения PCP.
- Порядковый номер для следующего входящего сообщения PCP.
- Данные из последнего исходящего сообщения.
- Интервал повтора передачи.
- Первичный сеансовый ключ (MSK) созданный с помощью EAP.
- Алгоритм MAC для транспортного ключа, который будет применяться при генерации подписи сообщений PCP.
- Псевдослучайная функция, согласованная при начальном обмене сообщениями PA-Server и PA-Client для создания транспортного ключа.
- Транспортный ключ, созданный на основе MSK для защиты целостности и аутентификации источника сообщений в сессии PA. Для транспортного ключа **следует** устанавливать срок действия, совпадающий с временем жизни сессии.
- Случайное значение nonce выбранное клиентом PCP при организации сессии.
- Идентификатор транспортного ключа (key ID).

  Транспортный ключ рассчитывается по формуле

  `prf(MSK, "IETF PCP" || Session ID || Nonce || key ID)`
  prf — псевдослучайная функция, указанная в опции PRF (параграф 5.7);

  MSK — первичный сеансовый ключ, созданный методом EAP;

  "IETF PCP" - ASCII-представление строки без завершающего null-символа (без кавычек);

  || - оператор конкатенации;

  Session ID — идентификатор сессии, для которой создан ключ MSK;

  Nonce — случайное значение, выбранное клиентом и переданное в начальном сообщении PA-Client;

  Key ID — идентификатор транспортного ключа.

5 Формат пакетов

5.1 Формат пакетов с сообщениями PCP Auth

Формат сообщения PA-Server идентичен формату отклика, описанному в параграфе 7.2 [RFC6887]. В качестве кода результата сообщения PA-Server с запросом EAP **должно** использоваться значение AUTHENTICATION_REQUEST.

Этот документ меняет трактовку поля Reserved (см. рисунок 1) в заголовке Request, описанного в параграфе 7.1 [RFC6887] для передачи данных, связанных с конкретной операцией.

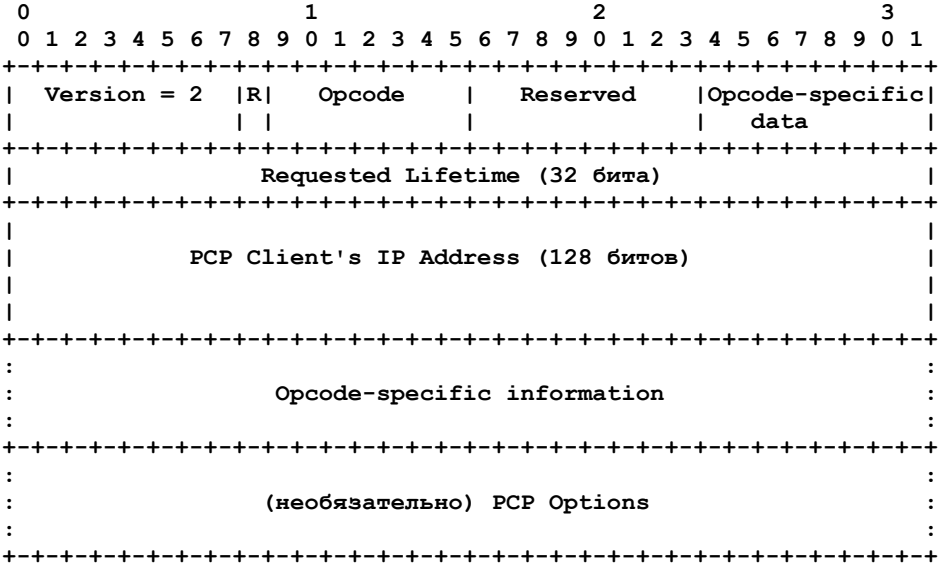


Рисунок 1. Формат пакета с запросом

В сообщениях PA-Client (рисунок 2) используется заголовок запроса, показанный на рисунке 1. Специфические для операции данные служат для передачи кода результата (например, INITIATION, AUTHENTICATION_FAILED). Остальные поля рисунка 2 описаны в параграфе 7.1 документа [RFC6887]. В качестве кода результата сообщений PA-Client с откликом EAP **должно** использоваться значение AUTHENTICATION_REPLY.

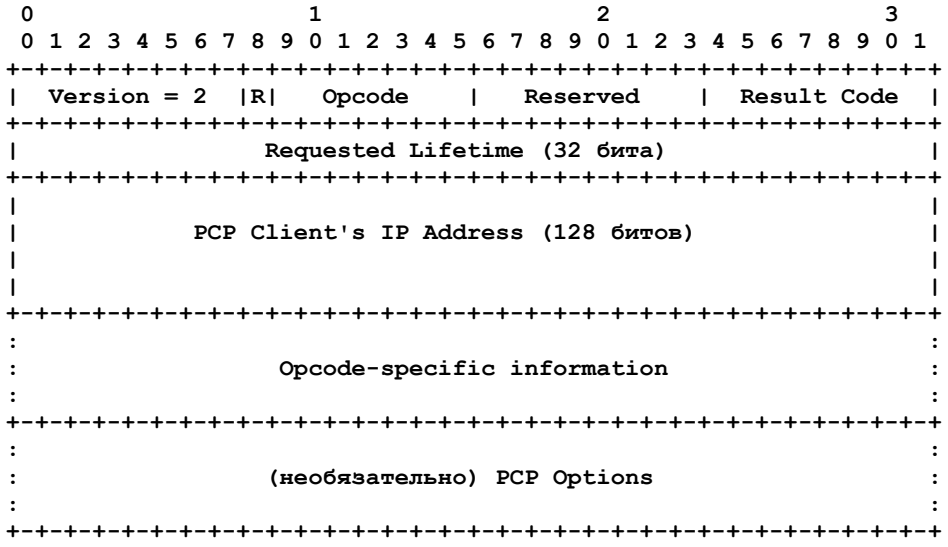
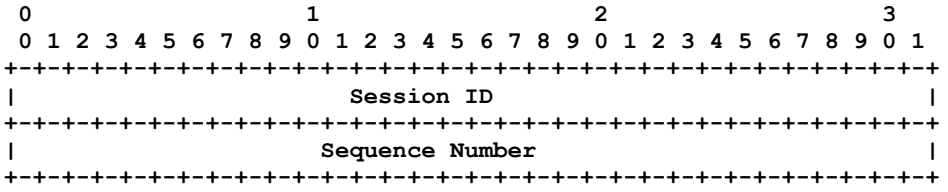


Рисунок 2. Формат сообщения PA-Client

Поля Lifetime в сообщениях PA-Client и PA-Server устанавливаются в 0 при передаче и игнорируются на приеме.

5.2 Данные операции AUTHENTICATION

Формат специфических для операции AUTHENTICATION данных показан ниже.



Session ID — идентификатор сессии

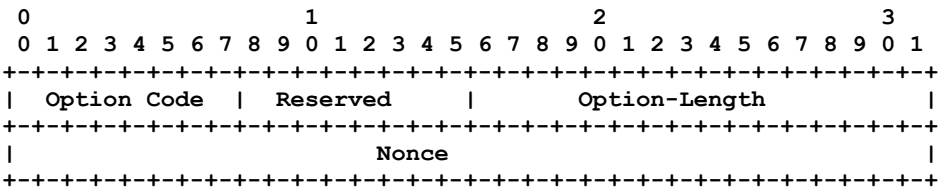
32-битовый идентификатор сессии PA.

Sequence Number — порядковый номер

32-битовый порядковый номер. Порядковый номер должен увеличиваться с каждым новым (не повторным) исходящим сообщением PA для обеспечения гарантий порядка сообщений PA.

5.3 Опция NONCE

Поскольку идентификатор сессии PA определяется сервером PCP, клиент PCP не знает идентификатора, который будет применяться, на момент отправки сообщения PA-Initiation. Для предотвращения атак с перехватом процесса аутентификации путем отправки обманных сообщений PA-Server клиенту PCP нужно указать случайное значение в поле nonce сообщения PA-Initiation. Сервер PCP будет добавлять это значение nonce в конец своего начального сообщения PA-Server. Если сообщение PA-Server не содержит корректного значение nonce, оно **должно** быть отброшено без уведомления.



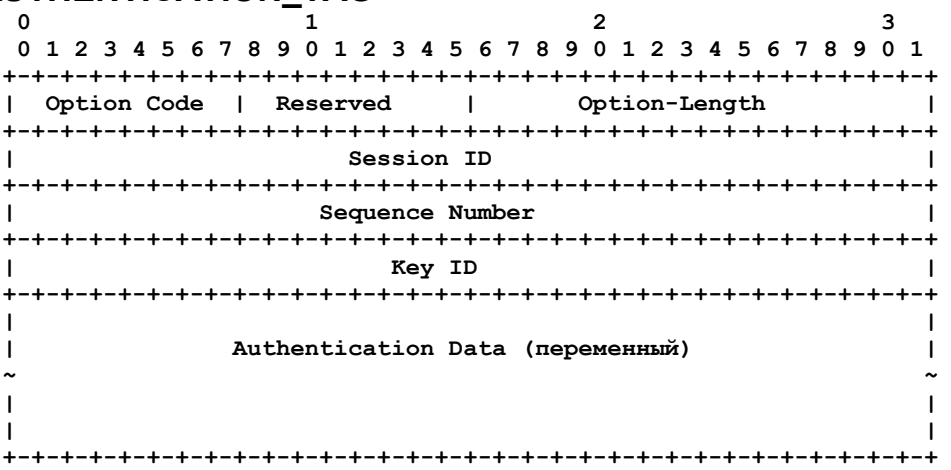
Option Code — код опции
4.

Reserved - резерв
8 битов, которые **должны** иметь значение 0 при передаче и **должны** игнорироваться на приеме.

Option-Length — размер опции
4 октета.

Nonce
Случайное 32-битовое значение, которое передается в сообщении PA-Initiation и соответствующем отклике сервера PCP.

5.4 Опция AUTHENTICATION_TAG



Поскольку в сообщениях PCP общего назначения код операции для аутентификации не предусмотрен, для передачи значений Session ID и Sequence Number в обычных сообщениях PCP используется специальный тег.

Option Code — код опции
5.

Reserved - резерв
8 битов, которые **должны** иметь значение 0 при передаче и **должны** игнорироваться на приеме.

Option-Length — размер опции
Размер опции AUTHENTICATION_TAG для обычного сообщения PCP (в октетах), включая 12-октетный заголовок и аутентификационные данные переменного размера.

Session ID — идентификатор сессии
32-битовое поле, используемое для идентификации сессии, к которой относится сообщение, а также секретного ключа, используемого для создания подписей, добавляемых в конец сообщения PCP.

Sequence Number — порядковый номер
32-битовый порядковый номер. В данной опции порядковый номер требуется инкрементировать для каждого нового (не повторного) обычного сообщения PCP для обеспечения упорядоченной доставки.

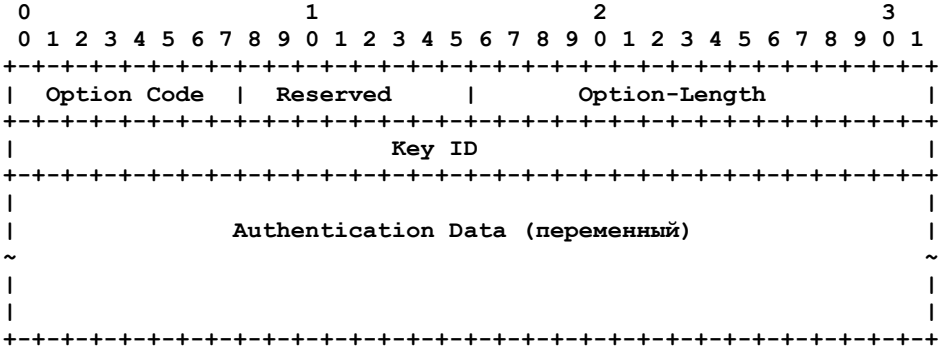
Key ID — идентификатор ключа
Идентификатор, связанный с транспортным ключом, который используется при генерации аутентификационных данных. Это поле заполняется нулями, если напрямую используется первичный ключ MSK.

Authentication Data — данные аутентификации
Поле переменного размера, в котором передается код аутентификации (MAC[1]) для обычного сообщения PCP. Генерация кода зависит от алгоритма, заданного в PCP SA. Поле **должно** заканчиваться на 32-битовой границе и при необходимости дополняется нулями.

5.5 Опция PA_AUTHENTICATION_TAG

Эта опция служит для аутентификации сообщений PA. В отличие от опции AUTHENTICATION_TAG для обычных сообщений PCP поля Session ID и Sequence Number не используются, поскольку соответствующая информация представлена в поле Opcode-specific information операции AUTHENTICATION.

[1]Message Authentication Code — код аутентификации сообщения.



Option Code — код опции

6.

Reserved - резерв

8 битов, которые **должны** иметь значение 0 при передаче и **должны** игнорироваться на приеме.

Option-Length — размер опции

Размер опции PA_AUTHENTICATION_TAG[1] для сообщения PCP Auth (в октетах), включая 4-октетный заголовок и аутентификационные данные переменного размера.

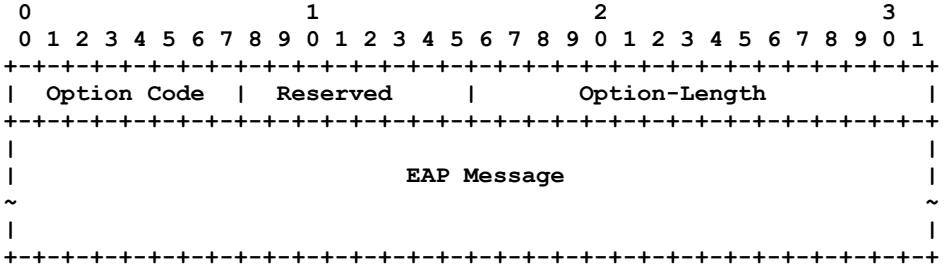
Key ID — идентификатор ключа

Идентификатор, связанный с транспортным ключом, который используется при генерации аутентификационных данных. Это поле заполняется нулями, если напрямую используется первичный ключ MSK.

Authentication Data — данные аутентификации

Поле переменного размера, содержащее код аутентификации (MAC) для сообщения PCP Auth. Генерация кода зависит от алгоритма, заданного в PCP SA. Поле **должно** заканчиваться на 32-битовой границе и при необходимости дополняется нулями.

5.6 Опция EAP_PAYLOAD



Option Code — код опции

7.

Reserved - резерв

8 битов, которые **должны** иметь значение 0 при передаче и **должны** игнорироваться на приеме.

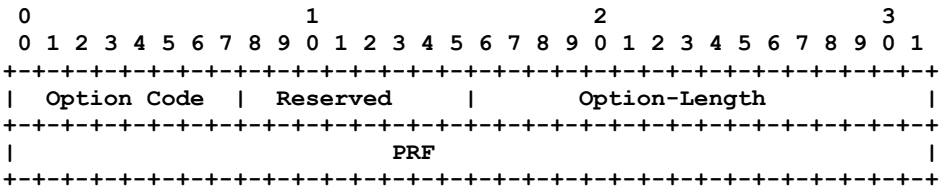
Option-Length — размер опции

Переменное значение.

EAP Message — сообщение EAP

Передаваемое в опции сообщение EAP. Поле **должно** заканчиваться на 32-битовой границе и при необходимости дополняется нулями.

5.7 Опция PRF



Option Code — код опции

8.

Reserved - резерв

8 битов, которые **должны** иметь значение 0 при передаче и **должны** игнорироваться на приеме.

Option-Length — размер опции

4 октета.

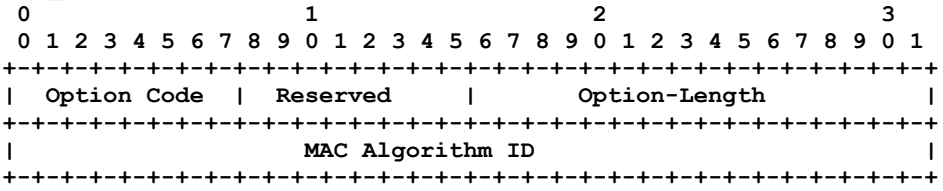
PRF — псевдослучайная функция

Псевдослучайная функция, которую отправитель использовал для генерации MSK. Это поле содержит значение, указывающее преобразование типа 2 протокола обмена ключами IKEv2[2] [RFC7296] [RFC4868]. Реализации PCP **должны** поддерживать PRF_HMAC_SHA2_256 (transform ID = 5).

[1] В оригинале опция ошибочно названа PA_AUTHENTICATION. См. https://www.rfc-editor.org/errata_search.php?eid=4513. *Прим. перев.*

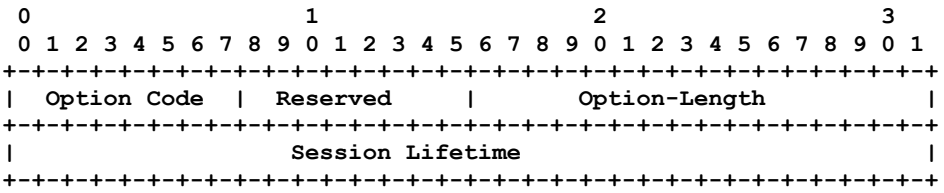
[2] Internet Key Exchange Protocol version 2 — протокол обмена ключами Internet версии 2.

5.8 Опция MAC_ALGORITHM



Option Code — код опции
9.
Reserved - резерв
8 битов, которые **должны** иметь значение 0 при передаче и **должны** игнорироваться на приеме.
Option-Length — размер опции
4 октета.
MAC Algorithm ID — идентификатор алгоритма MAC
Указывает алгоритм MAC, который отправитель использует для генерации аутентификационных данных. Поле MAC Algorithm ID содержит значение, указывающее преобразование типа 3 протокола обмена ключами IKEv2 [RFC7296] [RFC4868]. Реализации PCP **должны** поддерживать AUTH_HMAC_SHA2_256_128 (transform ID = 12).

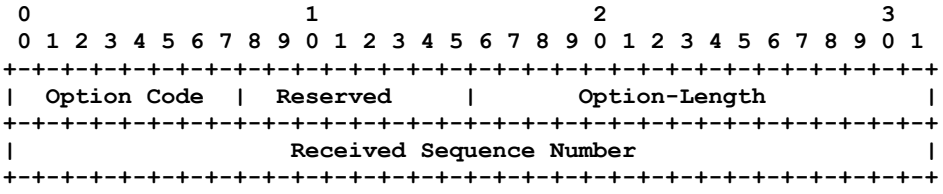
5.9 Опция SESSION_LIFETIME



Option Code — код опции
10.
Reserved - резерв
8 битов, которые **должны** иметь значение 0 при передаче и **должны** игнорироваться на приеме.
Option-Length — размер опции
4 октета.
Session Lifetime — срок действия сессии
32-битовое целое число из диапазона от 0 до 2^{32}-1, определяющее срок действия сессии PA в секундах.

5.10 Опция RECEIVED_PAK

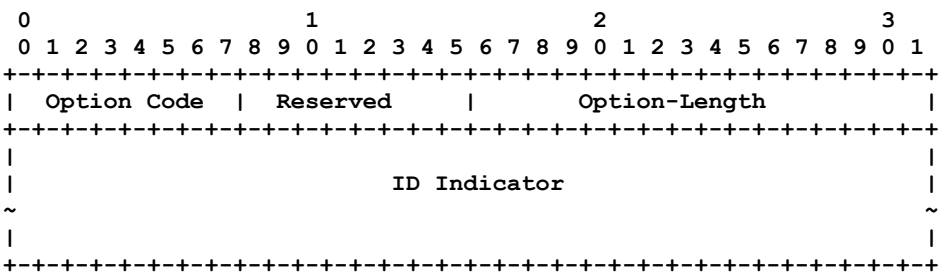
Эта опция используется в сообщениях PA-Acknowledgement для индикации приема сообщения PA с порядковым номером.



Option Code — код опции
11.
Reserved - резерв
8 битов, которые **должны** иметь значение 0 при передаче и **должны** игнорироваться на приеме.
Option-Length — размер опции
4 октета.
Received Sequence Number — полученный порядковый номер
Порядковый номер в последнем принятом сообщении PA.

5.11 Опция ID_INDICATOR

Опция ID_INDICATOR используется клиентом PCP для определения свидетельств, которые нужно предъявить серверу PCP.



Option Code — код опции
12.
Reserved - резерв

8 битов, которые **должны** иметь значение 0 при передаче и **должны** игнорироваться на приеме.

Option-Length — размер опции

Переменное значение.

ID Indicator — индикатор идентификатора

Идентифицирует орган, выдавший свидетельства EAP, которые будут применяться для аутентификации клиента. Это поле **недопустимо** завершать null-символом и его размер указывается в поле Option-Length. В частности, при получении клиентом опции ID_INDICATOR **недопустимо** трактовать наличие null-символа в качестве индикатора завершения поля ID Indicator.

Поле **должно** заканчиваться на 32-битовой границе и при необходимости дополняется нулями. В поле ID Indicator помещается строка в кодировке UTF-8 [RFC3629], соответствующая профилю UsernameCaseMapped для PRECIS IdentifierClass [RFC7613]. Клиент PCP проверяет соответствие поля ID Indicator профилю UsernameCaseMapped для PRECIS IdentifierClass. Клиент PCP применяет правила, приведенные в параграфе 3.2.2 [RFC7613] для отображения поля ID Indicator. Полученную в результате строку клиент PCP сравнивает с хранящимися локально идентификаторами для выбора используемых при аутентификации свидетельств. Две строки считаются при сравнении эквивалентными, если они совпадают в каждом октете.

6 Правила обработки

6.1 Генерация аутентификационных данных

После успешной аутентификации EAP все сообщения PCP в данной сессии PA **должны** включать тег аутентификации с подписью сообщения PCP для аутентификации источника и защиты целостности.

- Перед генерацией подписи для сообщения PA устройство сначала должно найти PCP SA, соответствующую идентификатору сессии и получить транспортный ключ. Далее устройство добавляет опцию PA_AUTHENTICATION_TAG в конец сообщения PCP Auth. Размер поля Authentication Data определяется алгоритмом MAC, выбранным для сессии. После этого устройство помещает в поле Key ID идентификатор транспортного ключа и устанавливает для поля Authentication Data значение 0. Затем устройство генерирует подпись для всего сообщения PCP (включая заголовок PCP и опцию PA_AUTHENTICATION_TAG), используя транспортный ключ и соответствующий алгоритм MAC. Полученное в результате значение помещается в поле Authentication Data.

- Подобно генерации подписи для сообщения PA перед генерацией подписи для обычного сообщения PCP устройство должно найти PCP SA, соответствующую идентификатору сессии и получает транспортный ключ. Далее устройство добавляет опцию AUTHENTICATION_TAG в конец сообщения PCP. Размер поля Authentication Data определяется используемым в сессии алгоритмом MAC. Далее устройство использует значения, полученные из SA для заполнения полей Session ID, Sequence Number и Key ID, а также устанавливает в поле Authentication Data значение 0. После этого устройство генерирует подпись для всего сообщения PCP (включая заголовок PCP и опцию AUTHENTICATION_TAG), используя транспортный ключ и соответствующий алгоритм MAC. Полученное в результате значение помещается в поле Authentication Data.

6.2 Проверка аутентификационных данных

Когда устройство получает обычное сообщение PCP с опцией AUTHENTICATION_TAG, оно должно использовать поле Session ID из этой опции для нахождения подходящей SA и получения соответствующего транспортного ключа (с использованием Key ID из опции) и алгоритма MAC. Если подходящей SA или транспортного ключа найти не удалось или не корректен порядковый номер (см. параграф 6.5), устройство PCP прекращает обработку сообщения и отбрасывает его без уведомления. После сохранения поля Authentication из опции AUTHENTICATION_TAG устройство заполняет поле Authentication нулями и генерирует подпись для сообщения (включая заголовок PCP и опцию AUTHENTICATION_TAG), используя транспортный ключ и алгоритм MAC. Если полученное значение подписи совпадает с сохраненным, устройство может быть уверено в том, что пакет не был подменен и проверка на этом завершается. Если значения не совпадают, устройство PCP прекращает обработку сообщения и отбрасывает его без уведомления.

Аналогичный процесс выполняется при получении сообщения PA с опцией PA_AUTHENTICATION_TAG для аутентификации PCP. Устройство должно использовать поле Session ID из Opcode для поиска соответствующей SA и получения транспортного ключа (с использованием Key ID из опции) и алгоритма MAC. Если подходящей SA или транспортного ключа не найдено или порядковый номер не корректен (см. параграф 6.4), устройство PCP прекращает обработку сообщения PCP и отбрасывает его без уведомления. После сохранения поля Authentication из опции PA_AUTHENTICATION_TAG устройство заполняет поле Authentication нулями и генерирует подпись для сообщения (включая заголовок PCP и опцию PA_AUTHENTICATION_TAG), используя транспортный ключ и алгоритм MAC. Если полученное значение подписи совпадает с сохраненным, устройство может быть уверено в том, что пакет не был подменен и проверка на этом завершается. Если значения не совпадают, устройство PCP прекращает обработку сообщения и отбрасывает его без уведомления.

6.3 Правила повтора передачи сообщений PA

Поскольку в обеспечении гарантированной доставки EAP полагается на нижележащие протоколы, после передачи сообщения PA клиенту/серверу PCP **недопустимо** передавать какие-либо последующие сообщения, пока от партнера не будет получено сообщение PA с подходящим порядковым номером. Если такого сообщения не будет получено, устройство PCP будет повторять передачу последнего сообщения в соответствии с правилами повтора. В данной спецификации используются правила повтора передачи, заданные в параграфе 8.1.1 базовой спецификации PCP [RFC6887]. В базовом протоколе PCP эти правила повтора применяются только клиентами PCP. Однако данная спецификация распространяет политику повтора и на серверы PCP. Если время максимальной продолжительности повторов (в секундах) истекло, а ожидаемого отклика не было получено, устройство будет прерывать сессию и отбрасывать текущую связь SA.

Как было указано в параграфе 3.1.3, для предотвращения неоправданных повторов получившее сообщение PA устройство **должно** передать его отправителю сообщение PA-Acknowledgement, если незамедлительная отправка

отклика PA не возможна. Сообщение PA-Acknowledgement подтверждает доставку сообщения PA. Получив сообщение PA-Acknowledgement, устройство прекращает повторы.

Отметим, что для сообщений PA, передаваемых в фазах инициирования сессии, ее повторной аутентификации или завершения, упомянутые выше правила не применяются, поскольку передающее сообщение устройство не ждет получения ответных сообщений PA.

Когда устройство получает повтор последнего входящего сообщения PA от своего партнера по сессии, оно **должно** попытаться повторить передачу последнего исходящего сообщения PA. Однако, если дубликат имеет тот же порядковый номер, но отличается от оригинального сообщения, устройство **должно** отбросить дубликат. Для решения этой задачи устройству может сохранение последнего входящего сообщения и связанных с ним ответных сообщений. Если для оригинала полученного дубликата еще не было отправлено ответных сообщений PA, устройство должно передать сообщение PA-Acknowledgement. Частота повтора откликов на дубликаты сообщений PA **должна** быть ограничена с целью обеспечения устойчивости к DoS-атакам[1].) Детали такого ограничения выходят за рамки данной спецификации.

6.4 Порядковые номера для сообщений PCP Auth

PCP использует для доставки сигнальных сообщений транспортный протокол UDP, который не обеспечивает гарантий доставки и сохранения порядка следования пакетов. Для обеспечения надежной доставки сообщений EAP при каждом обмене сообщениями PCP в процессе аутентификации EAP в сообщениях должны указываться монотонно возрастающие порядковые номера. В течение сессии PA устройство PCP должно поддерживать два порядковых номера для сообщений PA — один номер для входящих сообщений, другой для исходящих. При генерации исходящего сообщения PA устройство добавляет сохраненное значение порядкового номера в создаваемое сообщение и увеличивает хранящийся для этой SA порядковый номер на 1. При получении от партнера по сессии сообщения PA устройство не будет воспринимать данный пакет если содержащийся в нем порядковый номер не совпадает со входящим порядковым номером, сохраненным устройством. Если полученный порядковый номер корректен, устройство принимает сообщение и увеличивает хранящийся для данной SA входящий порядковый номер на 1.

Приведенные выше правила не применимы к сообщениям PA-Acknowledgement (сообщения PA с опцией RECEIVED_PAK). Сообщения PA-Acknowledgement не переносят каких-либо сообщений EAP и лишь подтверждают прием сообщений PA. Следовательно, гарантий доставки для сообщений PA-Acknowledgement не требуется. Например, после отправки сообщения PA-Acknowledgement устройство может сгенерировать отклик EAP. В этом случае устройство не имеет подтверждения доставки партнеру сообщения PA-Acknowledgement. Следовательно, при отправке или получении сообщения PA-Acknowledgement устройству **недопустимо** увеличивать значение порядкового номера, хранимого для данной SA, поскольку это преведет к рассогласованию порядковых номеров в случае потери PA-Acknowledgement.

Для сценария повторов сообщений имеется еще одно исключение. Как было отмечено в параграфе 6.3, если устройство PCP не получает какого-либо отклика от партнера по сессии, оно должно повторить последнее отправленное сообщение PA в соответствии с процедурой повтора, описанной в параграфе 8.1.1 [RFC6887]. Исходное сообщение и его дубликат должны быть идентичны (с точностью до бита). При получении устройством такого дубликата сообщения PA от партнера по сессии, оно **должно** заново передать свое последнее исходящее сообщение PA. В таких случаях повторная передача не ведет к изменению хранящихся порядковых номеров.

6.5 Порядковые номера для обычных сообщений PCP

При транспортировке обычных сообщений PCP в сессии PA устройству PCP требуется поддерживать порядковые номера для исходящих и входящих сообщений PCP. При генерации нового исходящего сообщения PCP устройство PCP помещает в поле Sequence Number в опции AUTHENTICATION_TAG хранящееся для данной SA значение исходящего порядкового номера и увеличивает хранимый номер на 1.

При получении сообщения PCP от партнера по сессии устройство PCP не будет воспринимать такой пакет, если порядковый номер в нем меньше сохраненного устройством значения входящего порядкового номера. Это обеспечивает защиту устройства PCP от атак с повторным использованием перехваченных пакетов (replay attack). При получении корректного порядкового номера устройство PCP воспринимает пакет и помещает номер из него в хранилище входящих порядковых номеров для данной PCP SA.

Отметим, что порядковый номер во входящем сообщении может не совпадать с хранящимся локально порядковым номером. Как отмечено в базовой спецификации PCP [RFC6887], если клиент PCP больше не заинтересован в транзакции PCP, но еще не получил отклика от сервера PCP, он прекращает повторы запросов PCP. После этого клиент может генерировать запросы PCP с иными целями, используя текущую связь SA. В таких случаях порядковые номера в новом запросе будут больше порядковых номеров в старом запросе и, следовательно, больше входящего порядкового номера, хранящегося на сервере PCP.

Отметим, что в соответствии с базовой спецификацией PCP [RFC6887] клиент PCP должен выбрать значение nonce для каждого запроса MAP или PEER и это значение nonce возвращается клиенту в отклике. Однако возможно использование клиентом одного значения nonce для множества запросов MAP или PEER что может создавать риск атак с повторным использованием пакетов. Эта проблема решается за счет использования порядковых номеров в откликах PCP.

6.6 Учет MTU

За обработку MTU отвечают методы EAP, поэтому в PCP не требуется специальных средств для обработки MTU. В частности, нижние уровни EAP показывают методы EAP, а также MTU серверов AAA[2] нижележащих уровней. Методы EAP (типа EAP-TLS [RFC5216], TEAP [RFC7170] и т. п.), в которых пакеты вероятно превосходят разумные значения MTU, поддерживают фрагментация и сборку фрагментов. Для прочих методов EAP (например, EAP-GPSK[3] [RFC5433]) предполагается, что размер пакетов никогда не превосходит значение MTU.

[1]Denial-of-service — атака на отказ служб.
[2]Authentication, Authorization, and Accounting — аутентификация, проверка полномочий и учет.
[3]Generalized Pre-Shared Key — обобщенный метод с известным заранее ключом.

Если сообщение EAP слишком велико для передачи в одном сообщении PA, оно будет делиться на части и передаваться в разных сообщениях PA. Отметим, что получатель может не знать, что делать далее, пока не получит все части и не соберет все сообщение EAP. В таких случаях для обеспечения гарантий доставки после приема сообщения PA получатель отвечает сообщением PA-Acknowledgement, служащим указанием для передачи следующего сообщения PA.

7 Согласование с IANA

Ниже приведен код операции PCP (PCP Opcode), выделенный из диапазона Standards Action в реестре PCP Opcodes, доступном по ссылке http://www.iana.org/assignments/pcp-parameters.

3 AUTHENTICATION - аутентификация

Ниже перечислены коды результатов PCP, выделенные из диапазона Standards Action в реестре PCP Result Codes, доступном по ссылке http://www.iana.org/assignments/pcp-parameters.

14 INITIATION - инициирование

Клиент включает этот код в запрос, направляемый серверу для аутентификации.

15 AUTHENTICATION_REQUIRED — требуется аутентификация

Отклик с таким кодом передается клиенту в тех случаях, когда требуется аутентификация EAP.

16 AUTHENTICATION_FAILED — отказ при аутентификации

Отклик для клиента об ошибке, связанной с отказом при аутентификации EAP.

17 AUTHENTICATION_SUCCEEDED — успешная аутентификация

Отклик, передаваемый клиенту после успешной аутентификации EAP.

18 AUTHORIZATION_FAILED — отказ при проверке полномочий

Отклик с таким кодом ошибки передается клиенту в тех случаях, когда аутентификация EAP прошла, но проверка полномочий (authorization) завершилась отказом.

19 SESSION_TERMINATED — сессия прервана

Этот код результата указывает партнеру на то, что сессия PA была прервана.

20 UNKNOWN_SESSION_ID — неизвестный идентификатор сессии

Отклик с таким кодом сервер PCP передает в случаях, когда он не обнаруживает сессии PA, связанной с полем Session ID в запросе PA или обычном запросе клиента PCP.

21 DOWNGRADE_ATTACK_DETECTED — обнаружена атака на снижение уровня

Этот код результата PCP показывает клиенту, что сервер обнаружил атаку с целью снижения уровня защиты.

22 AUTHENTICATION_REQUEST — запрос аутентификации

С помощью этого кода сервер показывает клиенту, что сообщение PA содержит запрос EAP.

23 AUTHENTICATION_REPLY — отклик при аутентификации

Клиенту показывает серверу, что сообщение PA содержит отклик EAP.

В последующих параграфах описаны опции PCP, выделенные из диапазона Standards Action реестра опций PCP, доступного по ссылке http://www.iana.org/assignments/pcp-parameters.

7.1 NONCE

Название:	NONCE.
Значение:	4.
Назначение:	см. параграф 5.3.
Используется с операцией:	AUTHENTICATION.
Размер:	4 октета.
Может присутствовать в:	запросах и откликах
Максимальное количество:	1.

7.2 AUTHENTICATION_TAG

Название:	AUTHENTICATION_TAG.
Значение:	5.
Назначение:	см. параграф 5.4.
Используется с операцией:	MAP, PEER, ANNOUNCE.
Размер:	переменный
Может присутствовать в:	запросах и откликах.
Максимальное количество:	1.

7.3 PA_AUTHENTICATION_TAG

Название:	PA_AUTHENTICATION_TAG.
Значение:	6.
Назначение:	см. параграф 5.5.
Используется с операцией:	AUTHENTICATION.
Размер:	переменный
Может присутствовать в:	запросах и откликах.
Максимальное количество:	1.

7.4 EAP_PAYLOAD

Название: EAP_PAYLOAD.

Значение: 7.

Назначение: см. параграф 5.6.

Используется с операцией: AUTHENTICATION.

Размер: переменный

Может присутствовать в: запросах и откликах.

Максимальное количество: 1.

7.5 PRF

Название: PRF.

Значение: 8.

Назначение: см. параграф 5.7.

Используется с операцией: AUTHENTICATION.

Размер: 4 октета.

Может присутствовать в: запросах и откликах.

Максимальное количество: с учетом максимального размера сообщений PCP.

7.6 MAC_ALGORITHM

Название: MAC_ALGORITHM.

Значение: 9.

Назначение: см. параграф 5.8.

Используется с операцией: AUTHENTICATION.

Размер: 4 октета.

Может присутствовать в: запросах и откликах.

Максимальное количество: с учетом максимального размера сообщений PCP.

7.7 SESSION_LIFETIME

Название: SESSION_LIFETIME.

Значение: 10.

Назначение: см. параграф 5.9.

Используется с операцией: AUTHENTICATION.

Размер: 4 октета.

Может присутствовать в: откликах.

Максимальное количество: 1.

7.8 RECEIVED_PAK

Название: RECEIVED_PAK.

Значение: 11.

Назначение: см. параграф 5.10.

Используется с операцией: AUTHENTICATION.

Размер: 4 октета.

Может присутствовать в: запросах и откликах.

Максимальное количество: 1.

7.9 ID_INDICATOR

Название: ID_INDICATOR.

Значение: 12.

Назначение: см. параграф 5.11.

Используется с операцией: AUTHENTICATION.

Размер: переменный.

Может присутствовать в: запросах.

Максимальное количество: 1.

8. Вопросы безопасности

Как описано в данной спецификации, после успешного завершения процесса аутентификации EAP между двумя устройствами PCP будет экспортироваться ключ MSK. Первичный ключ MSK служит для создания транспортных ключей, используемый при генерации MAC-подписей для последующих сообщений PCP. Однако до момента создания транспортного ключа сообщения PA в сессии PA имеют слабую криптографическую защиту и, если заранее между партнерами не был организован защищенный канал, такие сообщения могут послужить объектом MITM[1] или DoS-атак. Например, начальный обмен сообщениями PA-Server и PA-Client уязвим для атак с подменой (spoofing) поскольку для сообщений не используется аутентификации и защиты целостности. Кроме того, поскольку на этом этапе происходит обмен алгоритмами PRF и MAC, атакующий может предпринять попытку удаления опций PRF и MAC, задающих строгие алгоритмы, из начального сообщения PA-Server и вынудить клиента к выбору более слабых алгоритмов. Следовательно, серверам следует обеспечивать высокую надежность всех поддерживаемых ими алгоритмов PRF и MAC.

Для предотвращения простых DoS-атак устройствам PCP **следует** генерировать информацию о состоянии, как только это станет возможным для начальных сообщений PA-Server и PA-Client. Выбор метода EAP также очень важен. Выбранный метод EAP должен (1) быть устойчивым к атакам, которые возможны в незащищенной сетевой среде, (2) обеспечивать защиту от атак по словарю и (3) поддерживать организацию сеансовых ключей.

Если между сервером и клиентом размещается PCP-прокси [RFC7648], этот посредник может выполнять аутентификацию на сервере PCP до начала обработки клиентских запросов. Кроме того, повторная аутентификация между посредником и сервером не будет препятствовать обслуживанию клиентов, поскольку посредник может продолжать передачу серверу обычных сообщений PCP в процессе повторной аутентификации.

9 Литература

9.1 Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <http://www.rfc-editor.org/info/rfc3629>.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, DOI 10.17487/RFC3748, June 2004, <http://www.rfc-editor.org/info/rfc3748>.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, DOI 10.17487/RFC4868, May 2007, <http://www.rfc-editor.org/info/rfc4868>.

[RFC5281] Funk, P. and S. Blake-Wilson, "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)", RFC 5281, DOI 10.17487/RFC5281, August 2008, <http://www.rfc-editor.org/info/rfc5281>.

[RFC6887] Wing, D., Ed., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, DOI 10.17487/RFC6887, April 2013, <http://www.rfc-editor.org/info/rfc6887>.

[RFC7170] Zhou, H., Cam-Winget, N., Salowey, J., and S. Hanna, "Tunnel Extensible Authentication Protocol (TEAP) Version 1", RFC 7170, DOI 10.17487/RFC7170, May 2014, <http://www.rfc-editor.org/info/rfc7170>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <http://www.rfc-editor.org/info/rfc7296>.

[RFC7613] Saint-Andre, P. and A. Melnikov, "Preparation, Enforcement, and Comparison of Internationalized Strings Representing Usernames and Passwords", RFC 7613, DOI 10.17487/RFC7613, August 2015, <http://www.rfc-editor.org/info/rfc7613>.

[RFC7648] Perreault, S., Boucadair, M., Penno, R., Wing, D., and S. Cheshire, "Port Control Protocol (PCP) Proxy Function", RFC 7648, DOI 10.17487/RFC7648, September 2015, <http://www.rfc-editor.org/info/rfc7648>.

9.2 Дополнительная литература

[RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, DOI 10.17487/RFC5216, March 2008, <http://www.rfc-editor.org/info/rfc5216>.

[RFC5433] Clancy, T. and H. Tschofenig, "Extensible Authentication Protocol - Generalized Pre-Shared Key (EAP-GPSK) Method", RFC 5433, DOI 10.17487/RFC5433, February 2009, <http://www.rfc-editor.org/info/rfc5433>.

[RFC5448] Arkko, J., Lehtovirta, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", RFC 5448, DOI 10.17487/RFC5448, May 2009, <http://www.rfc-editor.org/info/rfc5448>.

Благодарности

Спасибо Dan Wing, Prashanth Patil, Dave Thaler, Peter Saint-Andre, Carlos Pignataro, Brian Haberman, Paul Kyzivat, Jouni Korhonen, Stephen Farrell и Terry Manderson за их полезные комментарии.

Адреса авторов

Margaret Cullen

Painless Security

356 Abbott Street

[1]Man-in-the-middle – атака, основанная на перехвате и изменении пакетов в пути с участием человека.

North Andover, MA 01845
United States
Phone: +1 781 405 7464
Email: margaret@painless-security.com
URI: http://www.painless-security.com

Sam Hartman
Painless Security
356 Abbott Street
North Andover, MA 01845
United States
Email: hartmans@painless-security.com
URI: http://www.painless-security.com

Dacheng Zhang
Beijing, China
China
Email: zhang_dacheng@hotmail.com

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India
Email: tireddy@cisco.com

Перевод на русский язык
Николай Малых
nmalykh@gmail.com