Содержание

RADIUS CoA 3
Виды нотификации CoA-Request 3
Упрощенная нотификация CoA-Request (запрос реавторизации) 3
Ответ на упрощенную нотификацию 4
Полная нотификация CoA-Request 5
Disconnect-Request 6
Настройка логики обработки DHCP абонента при получении PoD 6
Отдельные CoA-клиенты 9
Запрос accounting-сессии через CoA 9
Проверка существования сессии 10
Запрос accounting-сессии для данного IP-адреса 10
Запрос accounting-сессии по мульти-сессии 11

RADIUS CoA

CoA — Change of Authorization — это оповещения от RADIUS-сервера о том, что свойства пользователя поменялись или что пользователь стал неавторизованным. CoA-Request нотификация говорит о том, что пользователь авторизован и, опционально, у него изменились некоторые параметры. Таким образом, CoA-Request может приходить в следующих случаях:

- пользователь перешел из состояния "не авторизован" в состояние "авторизован" (например, пополнил счет) — см. далее;
- у авторизованного пользователя изменились параметры (подключение/отключение услуг, изменение профилей услуг).

Если пользователь не авторизован и изменяются его параметры, должен генерироваться упрощенный CoA-Request, который фактически инструктирует fastDPI произвести немедленную реавторизацию абонента, то есть послать Access-Request.

Виды CoA:

1. Упрощенный CoA-Request — при получении CoA fastDPI понимает, что атрибуты пользователя изменились и требуется повторная авторизация. Получив такое оповещение, fastDPI шлет обычный запрос `Access-Request` на RADIUS-сервер, как описано ранее.
2. Полный CoA-Request — оповещение `CoA-Request` может содержать полный список изменившихся атрибутов пользователя.
3. Disconnect-Request — сброс статуса авторизации пользователя.

Виды нотификации CoA-Request

Хотя оповещение `CoA-Request` может содержать полный список изменившихся атрибутов пользователя, предлагается использовать упрощенный вариант этой нотификации. Такой вариант говорит fastDPI, что атрибуты пользователя изменились и требуется повторная авторизация. Получив такое оповещение, fastDPI шлет обычный запрос `Access-Request` на RADIUS-сервер, как описано ранее.

Упрощенная нотификация CoA-Request (запрос реавторизации)

`CoA-Request` содержит следующие атрибуты:

- `Service-Type=8` (Authenticate-Only).
- `User-Name` — имя (логин) пользователя.
- Один из атрибутов `Framed-IP-Address`, `Framed-IPv6-Address`, `Framed-IPv6-Prefix` — IPv4 или IPv6-адрес абонента.
- `VasExperts-L2-SubsId` — идентификатор L2-абонента.

Предпочтительным идентификатором абонента в CoA является его логин. При обработке CoA fastDPI ищет абонента по логину (`User-Name` или `VasExperts-UserName`), если логин не найден — это ошибка. Если логин не указан в CoA, абонент ищется по IP-адресу. Если в CoA задан и логин, и IP-адрес, — IP-адрес игнорируется: fastDPI не анализирует, связаны ли логин и IP-адрес в базе данных UDR.

[CKAT 7.5+] Начиная с версии CKAT 7.5, возможно указывать атрибут `Acct-Session-Id` в качестве идентификатора абонента. CKAT ищет по `Acct-Session-Id` IP-адрес абонента у себя во внутренней БД и в случае успеха — формирует внутренний запрос реавторизации по IP. `Acct-Session-Id` является наиболее "слабым" из идентификаторов: он принимается во внимание только тогда, когда в CoA-запросе не указан ни логин, ни IP-адрес.

[CKAT 8.3+] Вместо атрибута `User-Name` можно указать логин абонента в атрибуте `Chargeable-User-Identity` (CUI). Чтобы CKAT поддержал CUI, необходимо в fastpcrf.conf указать

```
radius_attr_cui=1
```

Атрибут CUI не рекомендуется к использованию в CKAT, так как по RFC он содержит хеш логина абонента, а не сам логин. CKAT требует, чтобы CUI содержал истинный логин абонента.

Ответ на упрощенную нотификацию

Согласно RFC5176, на CoA-Request с Service-Type=8 (Authenticate-Only) должен быть ответ CoA-NAK с атрибутом Error-Cause=507 (Request Initiated). Это не всегда удобно, так как некоторые утилиты (например, radclient из FreeRADIUS) трактуют ответ CoA-NAK как ошибку. FastPCRF имеет настроечный параметр `coa_reauth_ack`, который определяет, как отвечать на CoA-Request с Service-Type=8:

- 0 — стандартное поведение: отвечать CoA-NAK с Error-Cause=507;
- 1 (значение по умолчанию) — отвечать CoA-ACK.

Этот параметр может быть задан в fastpcrf.conf как глобально, для всех RADIUS-серверов, так и для каждого RADIUS-сервера:

```
  # глобальная настройка
coa_reauth_ack=0

 # для этого сервера применяется глобальная настройка  coa_reauth_ack=0
radius_server=mysecret1@192.168.10.10%eth0
```

```
 # а для этого явно задано  coa_reauth_ack=1
radius_server=mysecret2@192.168.20.10%eth0;coa_reauth_ack=1
```

Полная нотификация CoA-Request

Хотя нотификация CoA-Request и поддерживается fastPCRF, но не рекомендуется к использованию из-за потенциальной сложности реализации: она должна содержать только изменения атрибутов (списка услуг и пр.) абонента.
Для авторизованного пользователя нотификация CoA-Request содержит только изменения параметров пользователя; поддерживаются следующие атрибуты:

- Имя (логин) пользователя — один из атрибутов `VasExperts-UserName`, `Chargeable-User-Identity` (CUI), `User-Name`.
- Один из атрибутов `Framed-IP-Address`, `Framed-IPv6-Address`, `Framed-IPv6-Prefix` — IPv4/IPv6-адрес; этот атрибут применяется только для поиска абонента, если логин не задан.
- `VasExperts-Multi-IP-User` — задает изменение признака, один или много IP-адресов связано с данным пользователем. Если пользователь становится многоадресным (то есть с одним пользователем может быть связано много IP-адресов), данный атрибут должен быть установлен в 1. Если пользователь становится одноадресным — данный атрибут должен быть установлен в 0. Если признак `multi-IP` пользователя не изменяется, CoA-Request не должен содержать атрибут `VasExperts-Multi-IP-User`. Допустимо не более одного данного атрибута в CoA-Request.
- `VasExperts-Policing-Profile` — имя профиля полисинга для пользователя. Данный атрибут должен включаться только если изменился профиль полисинга пользователя. В CoA-Request допустимо не более одного атрибута `VasExperts-Policing-Profile`. Если требуется удалить профиль полисинга у клиента, то следует послать атрибут `VasExperts-Policing-Profile` с пустым значением (с пустой строкой).
  [CKAT-9.6+] Согласно RFC 2865, строковые атрибуты не могут иметь пустого значения; поэтому начиная с версии 9.6 для удаления профиля полисинга у абонента следует указывать значение "n/a": `VasExperts-Policing-Profile=<n/a>`.
- `VasExperts-Enable-Service` — задает изменение статуса услуги: подключена (on) или отключена (off). В CoA-Request указываются все услуги, статус подключения которых изменился. Если какая-то услуга не содержится в CoA-Request, это значит, что статус её "подключенности" не изменился для пользователя. Каждая сменившая статус услуга должна задаваться отдельным атрибутом `VasExperts-Enable-Service`, то есть CoA-Request может содержать ноль или более атрибутов `VasExperts-Enable-Service`.
- `VasExperts-Service-Profile` — задает имя нового профиля услуги (то есть набор параметров услуги). Если данная услуга отключена, она включается (то есть `VasExperts-Service-Profile` имеет более высокий приоритет, чем `VasExperts-Enable-Service`). Для того чтобы отключить услугу с профилем, следует задать для неё атрибут `VasExperts-Enable-Service` со значением "off" (например, для услуги 5: `VasExperts-Enable-Service="5:off"`). Каждое изменение имени профиля услуги задается отдельным атрибутом `VasExperts-Service-Profile`, то есть CoA-Request может содержать ноль или более атрибутов `VasExperts-Service-Profile`.
- `Session-Timeout` — опциональный атрибут, задает время действия авторизации в секундах. Значение 0 игнорируется. По истечении этого времени статус авторизации пользователя устанавливается в "неизвестен", что приводит к отправке запроса на авторизацию Access-Request.

Disconnect-Request

Нотификация `Disconnect-Request` сигнализирует о том, что пользователь стал неавторизованным (например, закончились средства на счете). Нотификация Disconnect-Request может содержать следующие атрибуты:

- Один из атрибутов `Framed-IP-Address`, `Framed-IPv6-Address`, `Framed-IPv6-Prefix` — IPv4 или IPv6-адрес абонента.
- Имя (логин) пользователя — один из атрибутов `VasExperts-UserName`, `Chargeable-User-Identity` (CUI), `User-Name`.
- `Acct-Session-Id` — идентификатор accounting-сессии. По этому идентификатору CKAT ищет у себя во внутренней БД IP-адрес, связанный с данной accounting-сессией.
- `VasExperts-L2-SubsId` — идентификатор L2-абонента.

При получении Disconnect-Request CKAT:

1. если разрешен accounting — посылает Accounting Stop с причиной Admin-Reset (6);
2. для протоколов, допускающих разрыв сессии по инициативе сервера (например, PPPoE), — разрывает сессию;
3. проставляет статус авторизации для IP-адреса в статус "неизвестно". Это приводит к тому, что при поступлении пакета от данного IP CKAT пошлет запрос на авторизацию.

Если в Disconnect-Request указан логин абонента — эти действия производятся для всех IP-адресов, связанных с логином.

Если после PoD (CoA Disconnect) не пришло никакого DHCP-запроса до истечения lease time — такую сессию надо закрыть с отправкой деанонса и acct stop.
При этом следует учитывать, что у абонента может измениться тип сессии — вместо DHCP стать StaticIP или PPPoE; в этом DHCP-сессию нужно закрыть без деанонса и acct stop.

Настройка логики обработки DHCP абонента при получении PoD

Флаги опции `bras_dhcp_disconnect` используются для обеспечения гибкости в обработке PoD, так как между PoD и реавторизацией DHCP Discover от клиента может пройти достаточно много времени (max lease time / 2) и трафика:

- **0x0001** — `disable acct stop`, не посылать немедленно `acct stop` для `disconnected` DHCP-абонента. Позволяет учитывать трафик после PoD. По умолчанию acct-сессия закрывается по PoD, что может привести к неучтенному трафику для DHCP-абонентов от момента PoD до DHCP-реавторизации.
- **0x0002** — `disable L3 auth`, не выполнять L3-авторизации для `disconnected` DHCP-абонента. CKAT может авторизовать L2-абонента по его IP-адресу при поддержке RADIUS.

- **0x0004** — `block traffic` — блокируем весь трафик от `disconnected` абонента (то есть на пути `subs → inet`). Попытка сократить время реавторизации: многие CPE при пропадании соединения в Интернет досрочно шлют DHCP. Но цена этого флага — разрыв всех существующих сессий абонента.
- **0x0008** — на DHCP Request → отвечаем NAK. Позволяет сократить время реавторизации путем прерывания аренды IP-адреса.
- **0x0010** — игнорируем DHCP Request (ждем DHCP Discovery).

Эта опция покрывает следующие случаи:

`bras_dhcp_disconnect=0` (default, как сейчас):

- шлем acct stop
- следующий DHCP-запрос (Discover или Request) отправляется на RADIUS
- сбрасываем время L3-сессии, что приводит к L3 auth на первом не-DHCP-пакете от абонента

=1: ожидание DHCP-запроса от абонента без блокировки трафика, с L3 auth, без acct stop

- **не** шлем acct stop
- следующий DHCP-запрос (Discover или Request) отправляется на RADIUS
- сбрасываем время L3-сессии, что приводит к L3 auth на первом не-DHCP-пакете от абонента

=2, 3: ожидание DHCP-запроса от абонента без блокировки трафика, без L3 auth

- шлем (2) / не шлем (3) acct stop
- следующий DHCP-запрос (Discover или Request) отправляется на RADIUS

=4, 5: ожидание DHCP-запроса от абонента с блокировкой трафика, L3 enabled. То есть пакеты от абонента блокируются, но L3 auth по ним производится

- шлем (4) / не шлем (5) acct stop
- следующий DHCP-запрос (Discover или Request) отправляется на RADIUS
- сбрасываем время L3-реавторизации, что приводит к L3 auth на первом не-DHCP-пакете от абонента

=6, 7: (2 + 4) ожидание DHCP-запроса от абонента с блокировкой трафика, L3 disabled

- шлем (6) / не шлем (7) acct stop
- следующий DHCP-запрос (Discover или Request) отправляется на RADIUS
- трафик от абонента дропается

=8, 9: ожидание DHCP-запроса от абонента без блокировки трафика, L3 auth enabled

- шлем (8) / не шлем (9) acct stop
- сбрасываем время L3-реавторизации, что приводит к L3 auth на первом не-DHCP-пакете от абонента
- DHCP Request - отвечаем NAK, DHCP Discover - отправляем на RADIUS

=10, 11: (2 + 8) ожидание DHCP-запроса от абонента без блокировки трафика, L3 auth disabled

- шлем (10) / не шлем (11) acct stop
- DHCP Request - отвечаем NAK, DHCP Discover - отправляем на RADIUS
- L3 auth disabled

=12, 13: (4 + 8) ожидание DHCP-запроса от абонента с блокировкой трафика, L3 auth enabled. То есть пакеты от абонента блокируются, но L3 auth по ним производится

- шлем (12) / не шлем (13) acct stop
- DHCP Request - отвечаем NAK, DHCP Discover - отправляем на RADIUS
- трафик от абонента дропается
- сбрасываем время L3-реавторизации, что приводит к L3 auth на первом не-DHCP-пакете от абонента

=14, 15: (2 + 4 + 8) ожидание DHCP-запроса от абонента с блокировкой трафика, L3 auth disabled

- шлем (14) / не шлем (15) acct stop
- DHCP Request - отвечаем NAK, DHCP Discover - отправляем на RADIUS
- трафик от абонента дропается
- L3 auth disabled

=16, 17: ожидание DHCP-запроса от абонента без блокировки трафика, L3 auth enabled

- шлем (16) / не шлем (17) acct stop
- сбрасываем время L3-реавторизации, что приводит к L3 auth на первом не-DHCP-пакете от абонента
- DHCP Request - игнорируем (drop), DHCP Discover - отправляем на RADIUS

=18, 19: (2 + 16) ожидание DHCP-запроса от абонента без блокировки трафика, L3 auth disabled

- шлем (18) / не шлем (19) acct stop
- DHCP Request - игнорируем (drop), DHCP Discover - отправляем на RADIUS
- L3 auth disabled

=20, 21: (4 + 16) ожидание DHCP-запроса от абонента с блокировкой трафика, L3 auth enabled. То есть пакеты от абонента блокируются, но L3 auth по ним производится

- шлем (20) / не шлем (21) acct stop
- DHCP Request - игнорируем (drop), DHCP Discover - отправляем на RADIUS
- трафик от абонента дропается
- сбрасываем время L3-реавторизации, что приводит к L3 auth на первом не-DHCP-пакете от абонента

=22, 23: (2 + 4 + 16) ожидание DHCP-запроса от абонента с блокировкой трафика, L3 auth disabled

- шлем (22) / не шлем (23) acct stop
- DHCP Request - игнорируем (drop), DHCP Discover - отправляем на RADIUS
- трафик от абонента дропается
- L3 auth disabled

Все остальные значения `bras_dhcp_disconnect` являются ошибкой.

Данные acct stop все равно будут отправляться при любой авторизации (если в PCRF включена синхронизация auth/acct).
RADIUS понимает, что PoD обработался, получив Disconnect-ACK в ответ на PoD.

Отдельные CoA-клиенты

В некоторых конфигурациях CoA-клиент, посылающий CoA-запросы Disconnect-Request и CoA-Request, может быть отдельной сущностью, не являющейся RADIUS-сервером. Например, это может быть некая утилита, умеющая формировать CoA-запросы и применяющаяся в скриптах. FastPCRF поддерживает такие "обособленные" CoA-клиенты. В конфигурационном файле fastpcrf.conf каждый такой CoA-клиент задается отдельным параметром "coa_client", имеющим формат, аналогичный параметру `radius_server`:

```
coa_client=secret@ip%dev:port{;param=value}*
```

- `secret` — секрет RADIUS;
- `ip` — IP-адрес CoA-клиента;
- `dev` (необязательный) — имя интерфейса, на котором слушать входящие запросы; если не задан — интерфейс выбирается операционной системой;
- `port` — слушаемый локальный порт;
- `param=value` — перечень (через точку с запятой) конфигурационных параметров для данного CoA-клиента. Поддерживаются параметры: `max_resend_count`, `msg_auth_attr`, `coa_resend_timeout`.

Каждый CoA-клиент описывается в conf-файле отдельным параметром `coa_client`. Всего может быть до 16 обособленных CoA-клиентов. FastPCRF принимает CoA-запросы только от зарегистрированных (описанных в conf-файле) RADIUS-серверов и CoA-клиентов. Если RADIUS-сервер поддерживает CoA, нет необходимости описывать его ещё и параметром `coa_client`, — достаточно для этого RADIUS-сервера указать опцию `coa_port` в параметре `radius_server`.

Запрос accounting-сессии через CoA

[CKAT 8.2] Добавлена возможность запроса сторонней системой состояния accounting-сессии. Эта возможность реализована через CoA-Request с атрибутом `VasExperts-Command-Code=1`.

[CKAT 8.3] В связи с поддержкой мульти-сессий изменились логика работы и CoA-ответы.

Проверка существования сессии

CoA-Request со следующими атрибутами проверит, существует ли указанная accounting-сессия:

```
VasExperts-Command-Code=1
Acct-Session-Id=A1B2C3D4E5F6
```

В случае успеха возвращается CoA-ACK с указанием IP-адреса, к которому эта сессия относится:

```
# CoA-ACK атрибуты:
VasExperts-Command-Code=1
Acct-Session-Id=A1B2C3D4E5F6
    # CKAT-8.3: добавился атрибут ID мульти-сессий
Acct-Multi-Session-Id=MA1B2C3D4E5F6
    # CKAT-8.3: добавился атрибут NAS-IP-Address - каким fastDPI создана сессия
NAS-IP-Address=192.168.0.200
Framed-IP-Address=192.168.10.20
```

Если указанной сессии не существует (или она неактивна, например, завершена по idle timeout), возвращается CoA-NAK с атрибутами:

```
# CoA-NAK атрибуты:
VasExperts-Command-Code=1
Acct-Session-Id=A1B2C3D4E5F6
Error-Cause=503 # Session Context not found
# Атрибут Error-Cause может принимать и другие значения.
```

Запрос accounting-сессии для данного IP-адреса

Можно запросить у CKAT идентификатор активной accounting-сессии для данного IP-адреса. Структура запроса отличается для случаев "один fastPCRF — один fastDPI" и "один fastPCRF — несколько fastDPI".

Для случая "один fastPCRF — один fastDPI" CoA-Request выглядит так:

```
VasExperts-Command-Code=1
Framed-IP-Address=192.168.10.20
```

Для случая "один fastPCRF — несколько fastDPI" в CoA-Request нужно указать, какой fastDPI нас интересует:

```
# CoA-ACK атрибуты
VasExperts-Command-Code=1
Framed-IP-Address=192.168.10.20
    # CKAT-8.3: какой сервер fastDPI
NAS-IP-Address=192.168.0.200
```

В принципе, атрибут NAS-IP-Address (или NAS-Identifier) можно не указывать, если вы уверены, что данный IP-адрес есть только на одном fastDPI.

Если для указанного IP-адреса есть активная accounting-сессия, CKAT вернет CoA-ACK с идентификатором сессии:

```
# CoA-ACK атрибуты
VasExperts-Command-Code=1
Framed-IP-Address=192.168.10.20
Acct-Session-Id=A1B2C3D4E5F6
    # CKAT-8.3: добавился атрибут ID мульти-сессий
Acct-Multi-Session-Id=MA1B2C3D4E5F6
    # CKAT-8.3: добавился атрибут NAS-IP-Address - каким fastDPI создана сессия
NAS-IP-Address=192.168.0.200
```

Если активной сессии нет или же её нет на указанном fastDPI, вернется CoA-NAK вида:

```
# CoA-NAK атрибуты
VasExperts-Command-Code=1
Framed-IP-Address=192.168.10.20
Error-Cause=503 # Session Context not found
# Атрибут Error-Cause может принимать и другие значения.
```

CKAT 12.4 — Добавлена поддержка IPv6 для CoA.
Command-Code=1 — поиск acct session по IP.
Поиск acct-сессии может вестись по IPv6-префиксу атрибута Framed-IPv6-Prefix или Delegated-IPv6-Prefix. В ответе команды указываются все известные IP-адреса найденной acct-сессии — Framed-IP-Address, Framed-IPv6-Prefix, Delegated-IPv6-Prefix.

Запрос accounting-сессии по мульти-сессии

[CKAT 8.3] Можно по идентификатору мульти-сессии узнать, какому IP-адресу она соответствует и какая активная сессия у него есть для указанного fastDPI:

```
   # Атрибуты CoA-Request
VasExperts-Command-Code=1
Acct-Multi-Session-Id=MA1B2C3D4E5F6
```

Если данная мульти-сессия найдена, CKAT вернет IP-адрес, который соответствует данной мульти-сессии. В случае, если у мульти-сессии есть только одна активная сессия, вернется CoA-ACK:

```
# CoA-ACK атрибуты
VasExperts-Command-Code=1
Framed-IP-Address=192.168.10.20
Acct-Session-Id=A1B2C3D4E5F6
```

```
Acct-Multi-Session-Id=MA1B2C3D4E5F6
    # каким fastDPI создана сессия
NAS-IP-Address=192.168.0.200
```

Если нет активной сессии или же их более одной, вернется CoA-NAK с указанием IP-адреса абонента:

```
# CoA-NAK атрибуты
VasExperts-Command-Code=1
Acct-Multi-Session-Id=MA1B2C3D4E5F6
Framed-IP-Address=192.168.10.20
Error-Cause=503 # Session Context not found
# Атрибут Error-Cause может принимать и другие значения.
```

Можно в CoA-Request указать, какой fastDPI нас интересует:

```
   # Атрибуты CoA-Request
VasExperts-Command-Code=1
Acct-Multi-Session-Id=MA1B2C3D4E5F6
NAS-IP-Address=192.168.0.200
```

В этом случае CKAT вернет IP-адрес абонента и ID сессии, если для данного fastDPI есть активная сессия:

```
# CoA-ACK атрибуты
VasExperts-Command-Code=1
Framed-IP-Address=192.168.10.20
Acct-Session-Id=A1B2C3D4E5F6
Acct-Multi-Session-Id=MA1B2C3D4E5F6
    # каким fastDPI создана сессия
NAS-IP-Address=192.168.0.200
```

Если активной сессии для указанного fastDPI нет, CKAT вернет CoA-NAK:

```
# CoA-NAK атрибуты
VasExperts-Command-Code=1
Acct-Multi-Session-Id=MA1B2C3D4E5F6
NAS-IP-Address=192.168.0.200
Framed-IP-Address=192.168.10.20
Error-Cause=503 # Session Context not found
# Атрибут Error-Cause может принимать и другие значения.
```