

Содержание

PPPoE Radius Access-Request	3
1. Формат Access-Request	3
Поддержка PPPoE-опций circuit-id и remote-id	4
Поддержка Huawei vendor-specific tag 1	4
2. Формат Access-Accept	4
Время жизни сессии	6
3. Формат Access-Reject	6
Зачем для "наших" абонентов нужен Access-Reject?..	7

PPPoE Radius Access-Request

Авторизация PPPoE-сессий производится на Radius-сервере через сервер fastPCRF, см. [настройка fastPCRF](#). FastPCRF входит в СКАТ DPI и является по сути прокси между fastDPI и сторонним Radius-сервером.

Запросы Access-Request и ответы Access-Accept и Access-Reject отличаются от тех, что применяются в [L3-авторизации](#).

1. Формат Access-Request

Запрос Access-Request, формируемый fastPCRF, содержит следующие Radius-атрибуты:

- User-Name - для PAP/CHAP/MS-CHAPv2: логин абонента. Для авторизации по MAC-адресу этот атрибут содержит MAC-адрес абонента в виде строки, аналогично атрибуту Calling-Station-Id
- Password - пароль абонента (только для PAP-авторизации)
- CHAP-Challenge и CHAPPassword- для CHAP-авторизации
- MS_CHAP_Challenge и MS_CHAP2_Response (Microsoft VSA) - для MS-CHAPv2 - авторизации
- Calling-Station-Id - MAC-адрес абонента в виде строки, например, '01:02:e4:55:da:f5'. Используются маленькие буквы для hex-цифр A-F
- Acct-Session-Id - идентификатор accounting-сессии. Этот атрибут посылается всегда, даже если вы не используете accounting СКАТа.
- Service-Type = 2 (Framed)
- Framed-Protocol = 1 (PPP)

[СКАТ 7.6+] Если Access-Request инициирован [CoA-запросом реавторизации](#), то также добавляется атрибут Framed-IP-Address, содержащий выданный данному абоненту IP-адрес.

Атрибуты, идентифицирующие NAS (то есть СКАТ):

NAS-IP-Address, NAS-Identifier - IP-адрес или идентификатор fastdpi-сервера, задаваемый в параметре [fdpi_server](#). Отметим, что по умолчанию в Access-Request добавляется лишь один из атрибутов - NAS-IP-Address или NAS-Identifier, в зависимости от настроек [fdpi_server](#), приоритетным является [attr_nas_ip](#). Параметр [radius_add_all_nas_ids](#) позволяет добавлять в запрос оба этих атрибута:

```
# Разрешает добавлять атрибуты NAS-IP-Address И NAS-Identifier
# По RFC, в запросе может присутствовать либо NAS-IP-Address, либо NAS-
Identifier.
# Если заданы значения обеих опций, то приоритет отдается опции NAS-IP-Address.
# Значение данного параметра 1 разрешает добавлять оба атрибута в запрос.
#radius_add_all_nas_ids=0
```

VASExperts-Service-Type - Vendor-Specific атрибут, содержит число (int32), определяющее тип PPPoE-авторизации:

- VASExperts-Service-Type = 2 - для PAP
- VASExperts-Service-Type = 3 - для CHAP
- VASExperts-Service-Type = 4 - для MS-CHAPv2
- VASExperts-Service-Type = 5 - для авторизации по MAC-адресу

Message-Authenticator - [RFC2869] формируется, если в **fastpcrf.conf** параметр radius_msg_auth_attr=1

Если входящий пакет абонента содержит VLAN (то есть если у вас PPPoE-сеть с L2-тегами VLAN):

- NAS-Port-Type - настраивается в **fastpcrf.conf**, параметр radius_attr_nas_port_type, значение по умолчанию 5 (Virtual)
- NAS-Port - значение VLAN

Если входящий пакет абонента содержит QinQ (то есть если у вас PPPoE-сеть с L2-тегами QinQ):

- NAS-Port-Type - настраивается в **fastpcrf.conf**, параметр radius_attr_nas_port_type, значение по умолчанию 5 (Virtual)
- NAS-Port-Id - значение VLAN в виде строки формата "outerVLAN/innerVLAN", например, "10/102"

Поддержка PPPoE-опций circuit-id и remote-id

СКАТ начиная с версии 8.2 поддерживает PPPoE-опции circuit-id и remote-id согласно [RFC 4679](#). Значения этих опций передаются в Access-Request в VSA-атрибутах Agent-Circuit-Id и Agent-Remote-Id соответственно, vendor-id=3561.

Поддержка Huawei vendor-specific tag 1

СКАТ 12.4 — добавлена поддержка Huawei vendor-specific tag 1.

Значение интерпретируется как ADSL-Forum-Circuit-Id.

Если PPPoE-пакет содержит Circuit-Id и Huawei tag 1, то предпочтение отдается Circuit-Id, Huawei tag 1 игнорируется.

2. Формат Access-Accept

Ответ Access-Accept означает, что абонент авторизован, баланс достаточен, и ему выдан IP-адрес. Поддерживается dual stack: в одном ответе можно указать как IPv4-адрес и свойства абонента, так и IPv6-адрес, включая PD-префикс.



В СКАТ 8.4 реализована поддержка атрибута Framed-Pool: в ответе вместо Framed-IP-Address может быть указано имя пула, из которого следует выделить IP-адрес абоненту, подробнее см. [Локальный DHCP \(Пулы IP-адресов\)](#). Framed-IP-Address в нижеследующем описании следует читать так, что он



может быть получен из пула, а не быть явно указан в ответе Радиуса

Атрибуты:

- Framed-IP-Address - обязательный атрибут: IP-адрес, выданный абоненту.
- Idle-Timeout - необязательный атрибут: тайм-аут бездействия, в секундах. PPPoE-сессия будет закрыта, если в течение этого времени не было пакетов от/к абоненту. Если этот атрибут не задан, используется значение параметра `bras_ppp_idle_timeout` из `fastdpi.conf`
- Reply-Message - необязательный атрибут: сообщение, которое будет передано абоненту в PPP Auth-Ack ответе
- Session-Timeout - необязательный атрибут: max время жизни сессии, секунд.
- Acct-Interim-Interval - необязательный атрибут: период отправки промежуточных данных accounting'a, секунд (не может быть меньше 60). 0 - не отправлять промежуточный accounting.
 - ! Явное задание `Acct-Interim-Interval = 0` в ответе RADIUS отключает отправку Interim-Update.
- Class - необязательный атрибут: этот атрибут, если задан, будет отправляться "as is" во всех accounting-пакетах
- MS-CHAP2-Success - VSA-атрибут Microsoft [RFC2548], обязателен для MS-CHAPv2 авторизации

Поддерживаются следующие VSA-атрибуты Microsoft (vendor-id=311, RFC2548), все они не являются обязательными:

- MS-Primary-DNS-Server - IP-адрес primary DNS сервера
- MS-Secondary-DNS-Server - IP-адрес secondary DNS сервера
- MS-Primary-NBNS-Server - IP-адрес primary NetBios сервера
- MS-Secondary-NBNS-Server - IP-адрес secondary NetBios сервера

VSA-атрибуты VASExperts (vendor-id=43823), не являются обязательными:

[41] VASExperts-DHCP-DNS - IP-адрес DNS сервера. Может быть не более двух атрибутов VASExperts-DHCP-DNS: для основного (primary) и резервного (secondary) сервера.

Адреса DNS-серверов могут быть заданы через Microsoft VSA-атрибуты или VASExperts VSA-атрибут.

Поддержка IPv6: в одном ответе Access-Асцепт должны возвращаться как IPv4, так и IPv6-атрибуты. Поддерживаемые IPv6-атрибуты:

1. Framed-IPv6-Prefix - IPv6-префикс, выдаваемый абоненту. Длина префикса должна быть равна `ipv6_subnetwork`
2. Framed-IPv6-Address - IPv6-адрес абонента. СКАТ преобразует этот адрес в префикс, используя параметр `ipv6_subnetwork`
3. Delegated-IPv6-Prefix - PD-префикс, выдаваемый абоненту. Длина префикса должна быть равна `ipv6_subnetwork`
4. DNS-Server-IPv6-Address - IPv6-адрес DNS-сервера. Этих атрибутов может быть несколько - по одному для каждого DNS-сервера.
5. Framed-IPv6-Pool
6. Framed-IPv6-Route.

7. VSA-атрибуты для DHCPv6-опций

Кроме вышеперечисленных атрибутов, Access-Accept должен содержать профиль полисинга абонента и список подключенных услуг, см. [атрибуты свойств абонента](#)

Время жизни сессии

Если атрибута Session-Timeout в ответе нет, то PPPoE-сессия считается бессрочной и завершается либо по явному дисконнекту со стороны абонента, либо по тайм-ауту бездействия.

Если Session-Timeout указан, то СКАТ разорвет PPPoE-сессию по прошествии этого времени. Разрыв PPPoE-сессии четко описан в спецификациях PPP/PPPoE и заключается в отправке специальных term-сообщений абоненту; абонент, получив term, может создать новую PPPoE-сессию.

3. Формат Access-Reject

Возможно два типа "неавторизованности" абонента:

- абонент наш, но по какой-то причине (нулевой баланс, заблокирован и пр.) ему не может быть выдан полный спектр услуг
- абонент нам неизвестен - в этом случае абонента в сеть пускать нельзя

В первом случае (наш абонент) абоненту нужно выдать IP-адрес (то есть PPPoE-сессия будет установлена, авторизация успешна), но следует задать урезанные настройки - специальный профиль полисинга, услугу 5 (белый список + captive portal), - чтобы абонент смог зайти в сеть и, например, пополнить свой баланс. То есть Access-Reject должен содержать атрибут Framed-IP-Address для таких абонентов.

Во втором случае (левый абонент, ошибка в параметрах авторизации) пакет Access-Reject не должен содержать атрибута Framed-IP-Address, что трактуется как запрет входа в сеть: PPPoE-сессия не устанавливается, авторизация не проходит.

Access-Reject содержит следующие атрибуты:

- Framed-IP-Address - IP-адрес, выданный абоненту. Если абонент "левый", ему не надо выдавать IP-адрес, то есть атрибута Framed-IP-Address в Access-Reject быть не должно.
 - Idle-Timeout - тайм-аут бездействия, в секундах. PPPoE-сессия будет закрыта, если в течение этого времени не было пакетов от/к абоненту. Если этот атрибут не задан, сессия считается бессрочной (пока явно не будет закрыта абонентом)
 - Reply-Message - необязательный атрибут: сообщение, которое будет передано абоненту в PPP Auth-Ack/Auth-Nak ответе
 - Session-Timeout - необязательный атрибут: max время жизни сессии, секунд.
 - Acct-Interim-Interval - необязательный атрибут: период отправки промежуточных данных accounting'a, секунд (не может быть меньше 60). 0 - не отправлять промежуточный accounting.
- ❗ Явное задание Acct-Interim-Interval = 0 в ответе RADIUS отключает отправку Interim-Update.

- Class - необязательный атрибут: этот атрибут, если задан, будет отправляться "as is" во всех accounting-пакетах

Для типа авторизации MS-CHAPv2 поддерживается также атрибут MS-CHAP-Error [RFC2548].

Поддерживаются следующие VSA-атрибуты Microsoft (vendor-id=311, RFC2548), все они не являются обязательными:

- MS-Primary-DNS-Server - IP-адрес primary DNS сервера
- MS-Secondary-DNS-Server - IP-адрес secondary DNS сервера
- MS-Primary-NBNS-Server - IP-адрес primary NetBios сервера
- MS-Secondary-NBNS-Server - IP-адрес secondary NetBios сервера

VSA-атрибуты VASExperts (vendor-id=43823), не являются обязательными:

[41] VASExperts-DHCP-DNS - IP-адрес DNS сервера. Может быть не более двух атрибутов VASExperts-DHCP-DNS: для основного (primary) и резервного (secondary) сервера.

Адреса DNS-серверов могут быть заданы через Microsoft VSA-атрибуты или VASExperts VSA-атрибут.

Если абонент авторизован, то есть ему выдан IP-адрес, то в дополнение к вышеперечисленным атрибутам **обязательно** следует задать в специальных VASExperts VSA-атрибутах профиль полисинга VasExperts-Policing-Profile и профиль услуги 5 (белый список + Captive Portal) VasExperts-Service-Profile, подробнее см. [L3 BRAS](#).

Зачем для "наших" абонентов нужен Access-Reject?..

Профиль полисинга и услуги, заданные в Access-Reject, применяются временно. Если свойства абонента, пришедшие в атрибутах Access-Accept, запоминаются во внутренней базе данных (UDR) fastDPI и применяются даже после перезагрузки, то свойства из Access-Reject применяются без сохранения в UDR. То есть при перезагрузке fastDPI восстановятся те свойства абонента, которые пришли последний раз в Access-Accept, и fastDPI будет их применять до тех пор, пока не получит новые в ответ на Access-Request.