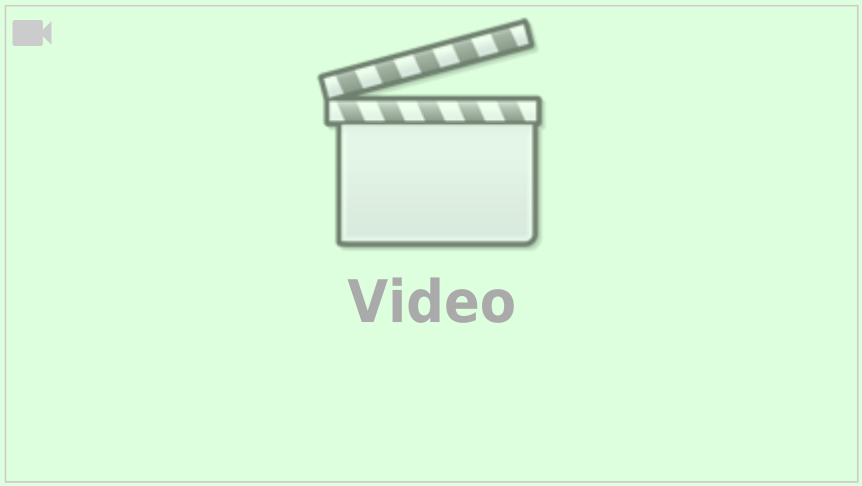
Table of Contents

Настройка PPPoE авторизации

Статья в блоге: PPPoE: особенности настройки, преимущества и отличия от других протоколов соединения

Обзор L2 PPPoE Mode:



FastDPI BRAS начиная с версии 7.2 поддерживает PPPoE. Для включения поддержки PPPoE необходимо:

1. Активировать BRAS
2. Задать в `fastdpi.conf`:

```
    # Включаем  PPPoE
bras_pppoe_enable=1
    # Задаем максимальное число  PPPoE-сессий
    # Рекомендуемое значение - в 1.5 - 2 раза больше числа  PPPoE-абонентов
bras_pppoe_session=10000

    # Обязательно должны быть заданы  IP  и MAC-адреса шлюза/бордера, расположенного за CKAT
    # (абонент -> CKAT -> бордер/шлюз)
bras_gateway_ip=192.168.0.1
bras_gateway_mac=aa:bb:cc:dd:ee:ff
```

Поддерживаются протоколы авторизации PAP, CHAP, MS-CHAPv2. Список разрешенных протоколов авторизации задается conf-параметром `bras_ppp_auth_list`. Протоколы в списке располагаются в порядке предпочтения: первый является самым предпочтительным.

Идентификаторы поддерживаемых протоколов:

- PAP - не рекомендуется к использованию
- CHAP-MD5
- MS-CHAPv2

Значение по умолчанию: все протоколы, кроме 1 (PAP):

```
bras_ppp_auth_list=2,3
```

Также возможна авторизация по MAC-адресу абонента, если в `fastdpi.conf` указано:

```
bras_ppp_mac_auth=1
```

Авторизация по MAC-адресу применяется, если сторонам не удалось договориться о протоколе авторизации.

- Дополнительные настройки PPPoE BRAS
- Авторизация PPPoE-сессий на Radius-сервера

Терминация PPPoE-трафика

При работе CKAT в режиме PPPoE-сервера (`bras_pppoe_enable=1`) производятся следующие манипуляции с PPPoE-пакетами:

- в направлении LAN → WAN: из пакета удаляются PPPoE/PPP заголовки, `srcMAC := bras_arp_mac`, `dstMAC := bras_gateway_mac`
- в направлении WAN → LAN: в пакет добавляются PPPoE/PPP заголовки, `srcMAC := bras_arp_mac`, `dstMAC := MAC-адрес` абонента. Если PPPoE сессия не найдена по IP, пакет дропается.

Все возможности по терминации трафика поддерживаются, включая VLAN/QinQ теги в PPPoE-трафике и их терминацию.

Параметр `bras_terminate_l2=1` к PPPoE-сессиям не применяется: для PPPoE всегда производится корректировка L2-заголовка пакетов как описано выше.

Режим терминации по AS к PPPoE-трафику не применим, так как в PPPoE-пакетах не всегда есть IP-адрес, поэтому определить AS в общем случае невозможно.

Обработка ARP в PPPoE

Со стороны абонентов ARP-запросы в PPPoE-сетях смысла не имеют, так как PPPoE - это соединение "точка-точка" и абонент может посылать пакеты только к PPPoE-серверу, MAC-адрес которого абоненту известен.

Со стороны WAN CKAT обрабатывает все ARP-запросы "Who is IP=x.x.x.x?", где x.x.x.x - IP-адрес "живого" PPPoE-абонента. В ответ CKAT возвращает значение параметра `bras_arp_mac`. То есть CKAT откликается на ARP-запросы к текущим PPPoE-сессиям.

Если PPPoE-абоненту подключена услуга NAT, ARP-запросы со стороны WAN к PPPoE-сессиям не обрабатываются

Для PPPoE-сессий поддерживаются все основные функции BRAS:

- IP source guard
- Замыкание локального трафика, в том числе разнородного, например, когда один сегмент является PPPoE-сетью, второй - DHCP-сетью

Восстановление PPPoE-сессий при рестарте CKAT

При старте fastDPI пытается восстановить PPPoE-сессии абонентов из UDR, чтобы кратковременный рестарт сервиса был незаметен для абонентов. Такое восстановление сессий для некоторых биллингов может приводить к рассогласованию состояния сессий в биллинге и CKAT, особенно при динамической раздаче IP-адресов: биллинг при выдаче адресов может руководствоваться последовательностью Access-Request + Acct-Start, тогда как при восстановлении сессии приходит только Acct-Start. В fastDPI 8.3 появилась возможность отключить восстановление PPPoE-сессий абонентов при старте: параметр `bras_pppoe_restore_on_startup` в `fastdpi.conf`:

```
    # Восстанавливать PPPoE-сессии на старте fastDPI
    # 1 (значение по умолчанию) - восстанавливать
    # 0 - не восстанавливать. Абоненты будут создавать новые сессии.
#bras_pppoe_restore_on_startup=1
```

Чтобы отключить восстановление PPPoE-сессий, следует явно задать `bras_pppoe_restore_on_startup=0` в `fastdpi.conf`. В этом случае абонент должен будет создать новую PPPoE-сессию и пройти авторизацию; при попытке обратиться к старой сессии CKAT будет посылать абоненту PADT-пакет терминации сессии.

Настройка Service-Name для VLAN

Тег Service-Name доступен с версии DPI 12.3!

Тег Service-Name необходим для установки процедуры авторизации согласно требованиям RFC, CKAT полностью поддерживает этот тег согласно всем требованиям.

Тег показывает, что далее следует имя сервиса. Поле TAG_VALUE представляет собой строку символов UTF-8 без завершающего NULL-символа. Нулевое значение поля TAG_LENGTH служит для индикации приемлемости любого сервиса. Примером использования тега Service-Name может служить индикация имени ISP2, класса или качества обслуживания.

Управление производится отдельно для каждого VLAN id.

Краткое руководство по управлению Service-Name можно вызвать командой

```
fdpi_cli help vlan group
```

Вывод свойств группы

Вывод всех свойств для всех групп:

```
fdpi_cli vlan group 0 show all
```

Вывод всех свойств для группы с конкретным id:

```
fdpi_cli vlan group <id> show all
```

Здесь id - номер VLAN, для которого нужно вывести информацию по Service-Name.

Пример:

```
fdpi_cli vlan group 1150 show all
```

Показать политику авторизации по PPPoE:

```
fdpi_cli vlan group <id> show auth pppoe
```

Показать политику для всех протоколов авторизации:

```
fdpi_cli vlan group <id> show auth all
```

Показать политику использования служебных имен для авторизации с помощью PPPoE:

```
fdpi_cli vlan group <id> auth pppoe show service-name all
```

Разрешение авторизации

Разрешить авторизацию через PPPoE в конкретном VLAN:

```
fdpi_cli vlan group <id> allow auth pppoe
```

Разрешить авторизацию через PPPoE для определенного Service-Name:

```
fdpi_cli vlan group <id> auth pppoe allow add service-name
name='<service_name>'
```

При установлении PPPoE-сессии на этапе Discovery stage после получения PADI пакета допустима временная задержка (параметр `delay`) перед отправлением PADO пакета. Допустимые значения параметра `delay`: 0, 1, 2, 3, 4, 5.

Разрешить авторизацию через PPPoE для определенного Service-Name с задержкой (измеряется в секундах):

```
fdpi_cli vlan group <id> auth pppoe allow add service-name
name='<service_name>' delay=<delay>
```

Пример:

```
fdpi_cli vlan group 1150 auth pppoe allow add service-name name='test1'
delay=5
```

Запрет авторизации

Чтобы запретить авторизацию для определенного VLAN, сначала нужно удалить все существующие правила для данного VLAN. То есть, чтобы разрешить определенные Service-Name, сначала нужно запретить все и только потом разрешить определенные теги.

Запретить авторизацию через PPPoE в конкретном VLAN:

```
fdpi_cli vlan group <id> deny auth pppoe
```

Запретить авторизацию через PPPoE для определенного Service-Name:

```
fdpi_cli vlan group <id> auth pppoe deny add service-name
name='<service_name>'
```

Пример: разрешаем авторизацию только определенным Service-Name:

```
fdpi_cli vlan group 1250 deny auth pppoe
fdpi_cli vlan group 1250 auth pppoe allow add service-name name='test2'
fdpi_cli vlan group 1250 auth pppoe allow add service-name name='test3'
delay=3
```

Пример: запрещаем авторизацию только определенным Service-Name:

```
fdpi_cli vlan group 350 allow auth pppoe
fdpi_cli vlan group 350 auth pppoe deny add service-name name='test-sname'
fdpi_cli vlan group 350 auth pppoe deny add service-name name='test-sname-
too'
```

При введении правил важна последовательность команд. Так, например, если ввести общий запрет авторизации после разрешающих правил, то авторизация с любым Service-Name в vlan 1250 будет недоступна:

```
fdpi_cli vlan group 1250 auth pppoe allow add service-name name='test2'
fdpi_cli vlan group 1250 auth pppoe allow add service-name name='test3'
delay=3
fdpi_cli vlan group 1250 deny auth pppoe
```

Данное ограничение распространяется и на одиночные запреты/разрешения.

Пример: разрешить авторизацию с Service-Name "test-sname".

```
fdpi_cli vlan group 350 auth pppoe deny add service-name name='test-sname'
fdpi_cli vlan group 350 auth pppoe allow add service-name name='test-sname'
```

Пример: запретить авторизацию с Service-Name "test-sname".

```
fdpi_cli vlan group 350 auth pppoe deny add service-name name='test-sname'
fdpi_cli vlan group 350 auth pppoe allow add service-name name='test-sname'
fdpi_cli vlan group 350 auth pppoe deny add service-name name='test-sname'
```

Другие команды

Удалить Service-Name и его свойства:

```
fdpi_cli vlan group <id> auth pppoe delete service-name
name='<service_name>'
```

Дроп трафика без анализа из конкретного VLAN:

```
fdpi_cli vlan group <id> drop
```

Дроп трафика с предварительным анализом, но без передачи в статистике Netflow из конкретного VLAN (Используется для работы с асимметричным трафиком, когда на площадку подается дубль трафика с другой площадки. Необходимо провести анализ и дропнуть трафик, чтобы он не попал в статистику):

```
fdpi_cli vlan group <id> hide
```

Пропуск трафика без какого-либо анализа из конкретного VLAN:

```
fdpi_cli vlan group <id> pass
```

Удалить все правила для всех заведенных VLAN (равносильно обработке VLAN по умолчанию):

```
fdpi_cli vlan group 0 delete all
```