# Содержание

Общая настройка BRAS для L2/L3 режимов	
Настройка BRAS L3 в fastDPI	
IPv6	
Внедрение BRAS-авторизации	
Параметры авторизации	
Hастройка BRAS L2 в fastDPI	
Настройка IPv6	
Включение IPv6 BRAS	8
Интеграция с Радиус-сервером	

# Общая настройка BRAS для L2/L3 режимов



Вебинар по теме:

# Hастройка BRAS L3 в fastDPI



Необходимо создать услуги и полисинг, которые в дальнейшем будут передавать с помощью Radius атрибутов от биллинга. Пример настройки полисинга (тарифный план) и Captive Portal, которые минимально необходимы для старта.

1. Создать файл aslocal.bin (или откорректировать этот файл, если он уже есть). В файл aslocal прописываются те диапазоны серых IP-адресов, которые используются в локальной сети провайдера. В качестве номера автономной системы для них указываем любой из диапазона 64512 – 65534.

vi aslocal.txt
10.0.0.0/8 64512
172.16.0.0/12 64512
192.168.0.0/16 64512
cat aslocal.txt | as2bin /etc/dpi/aslocal.bin



FastDPI авторизует только локальных пользователей. Локальность пользователя определяется по принадлежности его IP-адреса к списку локальных автономных систем.

2. Создать файл asnum.dscp (или откорректировать этот файл, если он уже есть). В этом файле нужно указать номера локальных (local) автономных систем – именно для них будет производиться авторизация. Как правило, это автономные системы для серых IP-адресов, указанные в aslocal.bin, плюс публичные IP-адреса, выделенные провайдеру, если эти публичные IP-адреса используются в локальной сети, то есть требуют авторизации. Для всех IP-адресов автономных систем, помеченных как local в asnum.dscp, будет производиться авторизация.

```
vi asnum.txt
64512 local
cat asnum.txt | as2dscp /etc/dpi/asnum.dscp
```

3. В /etc/dpi/fastdpi.conf активируем авторизацию:

```
enable_auth=1
```

4. Задать список fastPCRF-серверов:

```
auth servers=127.0.0.1%lo:29002,192.168.10.5%eth1:29002
```

Формат задания одного сервера: ip%dev:port, где ip - IP-адрес сервера, dev - локальное устройство, с которого устанавливать соединение. FastDPI устанавливает соединение с первым доступным сервером fastPCRF из списка.

**5.** Не забываем активировать UDR — хранилище свойств пользователей:

udr=1



После внесения изменений необходимо сделать перезапуск сервиса: service fastdpi restart.

#### IPv6

Для авторизации IPv6-адресов следует активировать поддержку IPv6. Фактически СКАТ авторизует не конкретный IPv6-адрес, а подсеть с заданной длиной префикса (по умолчанию /64). Например, если идут пакеты от адресов 2001:1::1 и 2001:1::10, то только один из этих адресов будет послан на авторизацию, а возвращенные параметры авторизации применяются для всех адресов из подсети 2001:1::/64.

Для IPv6 нет аналога файла aslocal.bin, так как нет приватных адресов. Вы должны пометить в файле asnum.dscp номера AS, которые требуют авторизации, как local.

Авторизация IPv6 автоматически включается, если в fastdpi.conf указано:

```
ipv6=1
enable_auth=1
```

Начиная с версии СКАТ 8.1.4 есть возможность принудительно отключить авторизацию IPv6адресов, указав в fastdpi.conf:

```
enable auth ipv6=0
```

Прочие настройки авторизации

# Внедрение BRAS-авторизации

Процесс внедрения нового функционала всегда труден и тернист, а в случае с BRASавторизацией - особенно, так как требует настройки не только fastdpi/fastpcrf, но и Radius-сервера, на котором происходит основная работа по авторизации абонентов, и всего backend'a за Radius-сервером, — базы данных, биллинговой системы и пр. Здесь мы рассмотрим несколько подходов к внедрению авторизации.

#### Тестовый стенд

Тривиальный и надежный способ — организовать тестовый стенд. Достоинства — не затронет живых абонентов, недостаток — нужно дополнительное оборудование. Не всегда возможно организовать полноценный стенд.

#### Отдельная автономная система

Как описано ранее, авторизация проводится только по локальным IP-адресам. Локальность IP-адреса задается флагом local для автономной системы. Отсюда вывод — можно выделить диапазон тестовых IP-адресов, задать им номер автономной системы из диапазона зарезервированных для частных целей (64512..65534), и прописать, что эта автономная система — локальная (local).

Таким образом, только IP-адреса, принадлежащие этой локальной автономной системе будут авторизоваться. "Живые" абоненты не будут затрагиваться до тех пор, пока автономные системы, к которым относится их IP-адреса, не будут объявлены как local. Это позволяет отлаживать авторизацию на боевом fastDPI.

### Тестовый ІР-адрес

Наконец, третья возможность, — объявить, что авторизацию нужно проводить только для указанных IP-адресов. Для этого в fastdpi.conf есть настройка auth\_trace\_ip, в которой можно задать один или два (но не более) IP-адреса:

```
auth_trace_ip=192.168.20.11,192.168.30.58
```

Указанные IP-адреса должны быть локальными (то есть относиться к автономной системе, объявленной как local, см. выше). В случае наличия настройки auth\_trace\_ip авторизация будет проводиться только для указанных в ней IP-адресов.

#### Параметры авторизации

B fastdpi.conf можно задать следующие параметры авторизации, в дополнение к описанным ранее:

auth\_resend\_timeout - тайм-аут перепосылки запросов к fastPCRF на авторизацию, в секундах. Значение по умолчанию: 60. Если fastDPI не получил в течение этого времени ответа от fastPCRF, то запрос авторизации будет повторен.

auth\_expired\_timeout - время жизни авторизации, **в минутах**. Значение по умолчанию 60 минут. Значение 0 - бессрочно. Этот параметр применяется только если в Radius-ответе нет атрибута Session-Timeout, который задает время жизни сессии. Отметим, что в Access-Reject атрибут Session-Timeout также может присутствовать. По истечении этого времени будет

послан повторный запрос авторизации.



Значение 0 (бессрочно) может привести к тому, что абонент, которому отказано в доступе (Access-Reject), останется в статусе "не авторизован" навечно. Вывести абонента из этого статуса можно только CoA-нотификацией на реавторизацию, рестартом fastDPI или вручную с помощью fdpi\_ctrl.

auth\_pcrf\_reconnect - тайм-аут реконнекта к fastPCRF, В секундах. Значение по умолчанию - 1 секунда.

#### Тестовые настройки

auth\_trace - булевый флаг, включающий трассировку авторизации, по умолчанию отключен. Следует учитывать, что трассировка авторизации очень сильно влияет на производительность fastDPI и активно пишет в логи, включать её без особой надобности не следует.

auth\_trace\_ip - список IP-адресов (не более двух), для которых следует проводить авторизацию. По умолчанию пустой.

Пример:

auth trace ip=192.168.10.20,192.168.30.45

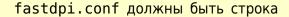
Этот список может быть применен на этапе внедрения авторизации и настройки Radiusсерверов: авторизация будет проводиться только по указанным локальным IP-адресам (обычно это тестовые абоненты), не затрагивая "живых" абонентов.

# Hастройка BRAS L2 в fastDPI

Активация функций BRAS в fastDPI производится следующими **обязательными настройками** конфигурационного файла fastdpi.conf:

- bras enable=1 общий флаг разрешения BRAS
- bras\_arp\_ip задает IPv4-адрес BRAS'a. Это может быть фейковый IP-адрес, не связанный ни с каким сетевым интерфейсом. Главное требование этот IP-адрес должен быть уникальным, никакому пользователю он не должен быть сопоставлен.
- bras\_arp\_mac MAC-адрес BRAS'a, формат XX:XX:XX:XX:XX, например, a0:00:b1:01:4e:cc. Этот MAC-адрес должен быть уникальным во всей локальной сети; это может быть фейковый MAC-адрес, не связанный ни с какой сетевой картой.
- auth\_servers задает список fastPCRF-серверов. Сервер fastPCRF отвечает за взаимодействие с Радиус-серверами. Формат задания одного сервера: ip%dev:port, где ip IP-адрес сервера, dev локальное устройство, с которого устанавливать соединение. FastDPI устанавливает соединение с первым доступным сервером fastPCRF из списка.







udr=1

#### Пример:

udr=1 auth\_servers=127.0.0.1%lo:29002 bras\_enable=1 bras\_arp\_ip=192.168.1.255

bras\_arp\_mac=a0:00:b1:01:4e:cc



При выборе значения параметра bras\_arp\_mac рекомендуется использовать существующий MAC-адрес порта карты. Но если используются улучшенные карты, например, 25G на чипе XXV710 или с драйвером i40e — можно поменять последний октет в MAC-адресе.

Пример: MAC-адрес порта карты — a0:00:b1:01:4e:cc, с измененным последним октетом — a0:00:b1:01:4e:dd.



Отдельные возможности fastDPI BRAS активируются дополнительными настройками, описанными далее, но без флага bras\_enable=1 этот дополнительный функционал будет недоступен.

# Настройка IPv6

L2 BRAS поддерживает выдачу IPv6-адресов stateful DHCPv6. В этом режиме IPv6-адрес абонентам выдается через DHCPv6. Автоматическое назначение IPv6-адресов (SLAAC/stateless DHCPv6) не поддерживается.

Концептуально схема работы выглядит так:

- 1. абонентский СРЕ ищет в сети IPv6-роутер с помощью ICMPv6. СКАТ анонсирует себя как IPv6-роутер, указывая, что для получения IPv6-адреса следует использовать DHCPv6;
- 2. СРЕ посылает DHCPv6-запрос получения IPv6-адреса;
- 3. СКАТ перехватывает все DHCPv6-запросы абонентов и обрабатывает их, тем самым фактически выступая как DHCPv6-сервер. Если абонент СКАТу неизвестен или его сессия истекла, DHCPv6-запрос транслируется в Радиус через PCRF;
- 4. PCRF получает ответ от Радиуса, содержащий, помимо прочих параметров, выданный абоненту IPv6-префикс и, если требуется, PD-префикс (prefix delegation), и транслирует этот ответ обрабно CKATy;
- 5. Получив от PCRF данные, CKAT посылает DHCPv6-ответ абоненту. CKAT выдает один IPv6адрес из выданного абоненту IPv6-префикса, а PD-префикс (если есть) передается абоненту полностью. Несмотря на то, что из IPv6-префикса выдается только один адрес, все IPv6-адреса этого префикса трактуются как адреса, принадлежащие этому абоненту. На самом деле абонент может запросить несколько IPv6-адресов, - все они будут выданы

из предоставленного IPv6-префикса.



Следует особо отметить, что Радиус должен выдавать абоненту IPv6-префикс фиксированной длины. Длина префикса задается параметром ipv6\_subnetwork, по умолчанию /64. Длина PD-префикса также должна равняться ipv6 subnetwork.

Если абоненту выдается и IPv6-префикс, и PD-префикс, то такой абонент обязательно должен быть помечен как multi-bind, так как с таким абонентом связано два IPv6-префикса; в ответе Радиуса должен быть атрибут VasExperts-Multi-IP-User=1.

#### Включение IPv6 BRAS

Режим IPv6 BRAS включается автоматически, если в fastdpi.conf задано

```
ipv6=1
bras_enable=1
```

Можно принудительно отключить IPv6 BRAS, указав в fastdpi.conf

```
bras ipv6=0
```

Параметр bras\_ipv6 является наполовину горячим: его можно отключить (bras\_ipv6=0) без рестарта СКАТа.

Режим обработки DHCPv6-запросов включается автоматически, если включен IPv6 BRAS. Можно принудительно запретить обработку DHCPv6 и ICMPv6 Router Solicitation, задав в fastdpi.conf

```
bras dhcp6 mode=0
```

Дополнительно в fastdpi.conf могут быть заданы следующие параметры:

- bras\_ipv6\_link\_local link-local (из FE80::/10) адрес СКАТ. Если данный параметр не задан, link-local адрес вычисляется автоматически из bras\_arp\_mac. СКАТ всегда имеет link-local адрес.
- bras\_ipv6\_address задает глобальный IPv6-адрес СКАТа. Глобальный адрес может быть полезен, например, для пингования СКАТа со стороны абонента. Если данный параметр не задан, СКАТ не имеет глобального IPv6-адреса.
- Опции ІСМРv6
- Опции DHCPv6

## Интеграция с Радиус-сервером

**Пример** запроса Access-Request на выдачу IPv6-префиксов абоненту:

```
Packet-Type = Access-Request
User-Name = "1106.106"
Calling-Station-Id = "a0:b1:c2:d3:00:6a"
Acct-Session-Id = "03119DF4AAB8E41D"
NAS-Identifier = "FastPCRF"
NAS-Port-Type = Virtual
NAS-Port-Id = "1106/106"
NAS-IP-Address = 188.227.73.40
VasExperts-Service-Type = DHCPv6
VasExperts-DHCPv6-Request = Solicit
VasExperts-DHCPv6-Delegated = 1
VasExperts-DHCP-ClientId = 0x00010001237d47fca0b1c2d3006a
```

В этом примере идентификатором абонента служит QinQ, запрос инициирован DHCPv6-пакетом Solicit (VasExperts-Service-Type = DHCPv6, VasExperts-DHCPv6-Request = Solicit), абонент запрашивает в том числе PD-префикс (VasExperts-DHCPv6-Delegated = 1).



Абонентское оборудование может запрашивать IPv6-адрес и PD-префикс в одном DHCPv6-запросе или же в разных. Поэтому полагаться на значение атрибута VasExperts-DHCPv6-Delegated не следует: даже если абонент не запрашивает PD-префикс, Радиус может выдать абоненту PD-префикс, СКАТ запомнит его и если CPE в будущем запросит PD-префикс, СКАТ возвратит ранее выданный абоненту PD

#### Пример ответа:

```
Packet-Type = Access-Accept
User-Name="abonent-106"
VasExperts-Multi-IP-User = 1
Framed-IPv6-Prefix = 2001:cafe:32:106::/64
Delegated-IPv6-Prefix = 2001:dele:32:106::/64
DNS-Server-IPv6-Address = 2001:feac::1
DNS-Server-IPv6-Address = 2001:feac::2
Session-Timeout = 7200
Idle-Timeout = 600
VasExperts-Policing-Profile = "rate_100M"
VasExperts-Service-Profile = "1:test1"
VasExperts-Enable-Service = "9:on"
VasExperts-Enable-Service = "12:on"
```

Здесь абоненту выдается два разных префикса:

- Framed-IPv6-Prefix = 2001:cafe:32:106::/64-из этого диапазона СКАТ будет выдавать IPv6-адреса абоненту
- Delegated-IPv6-Prefix = 2001:dele:32:106::/64-это delegated prefix передается
   СРЕ абонента (если, конечно, СРЕ запросит PD)

Следует обратить внимание на следующее:

- 1. в IPv6 адрес **всегда** должен быть связан с логином. Логин выступает как уникальный идентификатор абонента, с которым может быть связано множество IPv4-адресов и IPv6-префиксов. Логин абонента задается в ответе Access-Accept в атрибуте User-Name или VasExperts-UserName.
- 2. Если абоненту предоставляется несколько IPv6-префиксов (как в данном примере IPv6-префикс и PD-префикс), такой абонент **обязательно** должен быть помечен как multi-bind (атрибут VasExperts-Multi-IP-User = 1).

Атрибут Session-Timeout задает время сессии СКАТа (оно же - время accounting-сессии): в течение этого времени все DHCPv6-запросы от данного клиента СКАТ будет обрабатывать самостоятельно, возвращая ранее выданные Радиусом параметры. По прошествии Session-Timeout секунд текущая accounting-сессия закрывается и DHCPv6-запрос вновь транслируется в Радиус Access-Request. Если атрибута Session-Timeout нет в ответе Радиуса, он полагается равным fastdpi.conf-параметру auth expired timeout.

Время лизинга IPv6-префиксов задается fastdpi.conf-параметрами bras\_dhcp6\_preferred\_lifetime и bras\_dhcp6\_valid\_lifetime. Можно задавать время лизинга индивидуально для каждого абонента с помощью Радиус-атрибута DHCP-IP-Address-Lease-Time: этот атрибут задает preferred lifetime, valid lifetime полагается в два раза большим.

Дополнительные DHCPv6-опции могут быть заданы специальными VasExperts VSA атрибутами.

#### Задание DHCPv6-опций в Радиус

СКАТ поддерживает задание практически любой DHCPv6-опции через специальные VSA-атрибуты VasExperts. Если установка СКАТ производилась штатными средствами из официального репозитория VasExperts, то актуальный словарь всех VSA VasExperts находится в файле /usr/share/dpi/dictionary.vasexperts. Все эти атрибуты являются строковыми с единым форматом значения:

```
opt:value
```

где opt - число, идентификатор опции, value - значение опции.

VSA атрибут	Описание
VasExperts-DHCP-Option-IPv6	Опции, задающие IPv6-адрес или список IPv6- адресов
VasExperts-DHCP-Option-IPv6-Prefix	Опции, задающие IPv6-префикс
VasExperts-DHCP6-Option-Num	Задает опцию с числовым значением
VasExperts-DHCP6-Option-String	Задает опцию со строковым значением
VasExperts-DHCP6-Option-Bin	Задает бинарную опцию в виде hex-строки. Следует учитывать, что при задании бинарной опции её значение должно быть в network byte order

#### Пример (в формате FreeRadius):

```
# Опция 22 - список IPv6-адресов SIP-серверов:

# СКАТ пошлет в DHCPv6 одну опцию 22 со значением - список указанных IPv6 адресов

&VasExperts-DHCP-Option-IPv6 := "22:2c0f:ff91::10:1"

&VasExperts-DHCP-Option-IPv6 += "22:2c0f:ff91::10:2"
```

```
# Опция 71 - MIPv6 Home Network Prefix Option
  # задает IPv6-префикс
&VasExperts-DHCP-Option-IPv6-Prefix += "71:2c0f:ff90:71::/56"
  # Опция 32 - OPTION INFORMATION REFRESH TIME, числовая:
&VasExperts-DHCP6-Option-Num += "32:55779"
  # Опция 27: IPv6-адрес NIS-сервера, заданная в бинарном виде
# то же самое может быть задано так:
 # &VasExperts-DHCP-Option-IPv6 += "27:2c0f:ff91::20:1
 # Опция 43: ERO (Relay Agent Echo Request option)
 # приведена в качестве примера задания опции, значение которой - список чисел
  # СКАТ объединит все атрибуты по 43 опции в одну DHCPv6-опцию со значением '50,60,32'
&VasExperts-DHCP6-Option-Num += "43:50"
&VasExperts-DHCP6-Option-Num += "43:60"
 # int16-опция в бинарном виде (значение 32)
&VasExperts-DHCP6-Option-Bin += "43:0020"
```

Полный актуальный список всех DCHPv6-опций вместе со ссылками на RFC можно найти на сайте IANA.

### ICMPv6 настройки fastDPI

B fastdpi.conf могут быть заданы следующие параметры обработки ICMPv6 Router Solicication/Advertisement; большинство из этих параметров определены в RFC 4861:

Параметр	Формат	Значение по умолчанию	Описание
bras_ipv6_router_pref	число	0	Режим и приоритеты BRAS как IPv6- роутера: -1 - BRAS не является IPv6-роутером, то есть не обрабатывает ICMPv6 Router Solicitation и не шлет Router Advertisement; 0 - BRAS является IPv6-роутером с приоритетом Medium; 1 - BRAS является IPv6-роутером с приоритетом High; 3 - BRAS является IPv6-роутером с приоритетом Low
bras_icmp6_rtradv_mtu	число	1500	MTU, указываемый в Router Advertisement. Значение 0 - не добавлять MTU-опцию в Router Advertisement

Параметр	Формат	Значение по умолчанию	Описание
bras_icmp6_reachable_time	число	0	AdvRetransTimer, в миллисекундах. Используется IPv6-клентами - время между ретрансмитом Neighbor Solicitation сообщений. <b>0</b> - не задается роутером
bras_icmp6_hop_limit	число	64	AdvCurHopLimit значение поля Нор Limit IPv6-пакетов
bras_icmp6_default_lifetime	число	1800	AdvDefaultLifetime, в секундах. Используется IPv6-клиентами для построения списка default routers. Значение 0 говорит о том, что BRAS не является default router'ом.

### **Unsolicited RA**

Так как CKAT в режиме L2 BRAS является IPv6-роутером, он должен, согласно RFC 4861, периодически анонсировать себя в локальную сеть посредством сообщения ICMPv6 Router Advertisement (unsolicited RA). Для включения периодических анонсов предназначены следующие параметры fastdpi.conf:

Параметр	Формат	Значение по умолчанию	Описание
bras_icmp6_send_rtradv	число	0	Посылать (1) или нет (0) периодический RA
bras_icmp6_min_rtradv_interval	число	200	Начальная граница интервала отправки периодического RA, секунд
bras_icmp6_max_rtradv_interval	число	600	Конечная граница интервала отправки периодического RA, секунд

При включенном режиме отправки unsolicited RA время следующей отправки RA выбирается случайным образом из интервала [bras\_icmp6\_min\_rtradv\_interval, bras\_icmp6\_max\_rtradv\_interval] для каждого активного DHCPv6-абонента.

## DHCPv6 настройки fastDPI

B fastdpi.conf могут быть заданы следующие параметры обработки DHCPv6:

Параметр	Формат	Значение по умолчанию	Описание
bras_dhcp6_enable_rapid_commit	число	0	разрешен или запрещен Rapid Commit. Обычная процедура выдачи адреса в DHCPv6 состоит из 4 шагов (2 запроса + 2 ответа). Можно использовать 2-шаговую процедуру (Rapid Commit):  0 - запретить Rapid Commit; 1 - разрешить Rapid Commit. 2-шаговая процедура выдачи адреса будет применяться только для клиентов, которые поддерживают Rapid Commit
bras_dhcp6_enable_unicast	число	0	разрешен или запрещен Server Unicast <b>0</b> - unicast запрещен. Unicast- запросы DHCPv6 со стороны клиента будут игнорироваться. <b>1</b> - unicast разрешен.
bras_dhcp6_preferred_lifetime	число	3600	Предпочтительное время аренды IPv6-адреса, секунд. Это значение должно быть меньше, чем bras_dhcp6_valid_lifetime
bras_dhcp6_valid_lifetime	число	7200	Время аренды IPv6-адреса, секунд. Это значение должно быть больше, чем bras_dhcp6_preferred_lifetime.
bras_dhcp6_preference	число	-1	Значение Preference-опции в DHCPv6 Advertise. Эта опция задает предпочтительность DHCPv6-сервера в сети с несколькими DHCPv6-серверами1 - не указывать Preference-опцию в DHCPv6 Advertise.
bras_dhcp6_nak_lifetime	число	60	[СКАТ 8.3] Время жизни Reject- ответа Радиуса, секунд Если Радиус не выдал клиенту IPv6- адреса, клиент может повторять DHCPv6-запросы бесконечно и весьма часто, вызывая тем самым шторм Access-Request запросов на Радиус. Данным параметром можно задать период времени, в течение которого СКАТ сам будет отвечать на запросы тех клиентов, которым Радиус не выдал IPv6-адрес.