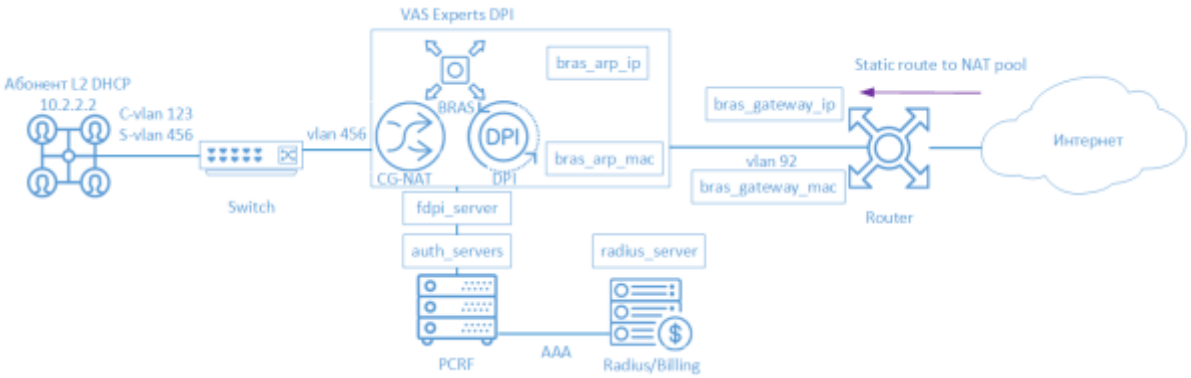
Table of Contents

Пример BRAS L2 ARP



BRAS ARP L2 означает, что абонент настраивает IP-адрес статично на своем устройстве и проходит AAA в Биллинге при отправке ARP запроса к своему шлюзу по умолчанию (также возможна схема, когда абонентам выдается префикс /30). Дальше терминируется CKAT и попадает на бордер.

Для организации работы CKAT в режиме BRAS L2 ARP участвуют следующие элементы:

1. Клиент с типом доступа Q-in-Q
2. FastDPI - обработка трафика и применение политик
3. FastPCRF - проксирование запросов между fastDPI и Radius
4. Radius сервер - принимает запросы от fastPCRF и формирует ответы с заданными атрибутами
5. Router - отвечает за передачу пакетов в интернет и обратный маршрут, на текущий момент возможен сценарий со Static Route и сценарий с настройкой маршрутизации OSPF и BGP на CKAT

Сценарий

Настройка FastDPI

Редактирование файла конфигурации DPI

Сперва необходимо раскомментировать (добавить) следующие строчки в файл конфигурации */etc/dpi/fastdpi.conf* .

```
  #включение внутренней базы данных свойств пользователей
udr=1
  #включаем режим авторизации по IP
enable_auth=1
  #активирует режим L2 BRAS
bras_enable=1

  #"виртуальный" IP адрес DPI (должен быть уникальным в сети)
```

```
bras_arp_ip=192.168.1.2
  #"виртуальный" MAC адрес DPI (следует использовать рельный MAC адрес любого из
DNA интерфейсов)
bras_arp_mac=a0:36:9f:77:26:58

    #IP адрес бордера
bras_gateway_ip=192.168.1.1
    #MAC адрес интерфейса, в который подключен DPI, на бордере
bras_gateway_mac=c4:71:54:4b:e7:8a

  #данные сервера, где установлен Fastpcrf (если на том же, где и Fastdpi, не
изменять)
auth_servers=127.0.0.1%lo:29002

  #включаем октлик на ARP-запросы к шлюзам
bras_arp_proxy=0x0002
  #включаем авторизацию по ARP запросам
bras_arp_auth=2

  #терминация vlan (в данном случае тэг будет вырезан)
bras_vlan_terminate=1
  #замыкание локального трафика
bras_terminate_local=1

  #включение accounting
enable_acct=1
  #статистика по биллингу абонента
netflow=4
  #тайм-аут отправки статистики
netflow_timeout=60
```

Следует выставить **свои** значения для следующих параметров

- bras_arp_ip
- bras_arp_mac
- bras_gateway_ip
- bras_gateway_mac

Настройка FastPCRF

Необходимо настроить FastPCRF. Для этого редакитурем файл */etc/dpi/fastpcrf.conf* . Находим строчку с параметрами RADIUS сервера и изменяем

```
    #secret123 - Radius секрет
    #192.168.1.10 - IP адрес Radius сервера
    #eth0 - интерфейс, **с которого** FastPCRF "общается" с Radius сервером
  #1812 - порт, на который FastPCRF отправляет запросы авторизации
```

```
     #acct_port - порт, на который FasPCRF отправляет Accouting
radius_server=secret123@192.168.1.10%eth0:1812;acct_port=1813
```

Настройка Radius

Настройка приводится в качестве **примера** на freeRADIUS 3 и может отличаться от конфигурации Вашего Radius сервера.

Словарь VasExperts

Сперва необходимо добавить VSA словарь

- копируем словарь /usr/share/dpi/dictionary.vasexperts из дистрибутива fastpcrf в каталог $freeRadius/share/freeradius
- Добавляем в главный словарь $freeRadius/share/freeradius/dictionary строку:

```
$INCLUDE dictionary.vasexperts
```

Создание Radius клиента

Добавляем в raddb/clients.conf Radius-сервера следующие строки

```
client fastdpi1 {
    ipaddr        = 192.168.1.5
    secret        = secret123
    require_message_authenticator = yes
#   add_cui = yes
    virtual_server    = fastdpi-vs
}
```

Создание виртуального сервера

Для создания конфигурации виртуального сервера копируем файл raddb/sites-available/default, входящий в поставку FreeRadius, в raddb/sites-enabled/fastdpi-vs и затем редактируем fastdpi-vs:

- задаем имя виртуального сервера - меняем в начале файла строку server default на server fastdpi-vs
- в секции listen для auth-запросов (type = auth) прописываем, на каком IP-адресе и каком порту слушать входящие запросы (заметим, это локальный адрес Radius-сервера):

```
ipaddr = 192.168.1.10
port = 1812
interface = eth0
```

Создание учетной записи для авторизации

Добавляем в файл */etc/raddb/users* данные по абоненту (следует учесть, что FastPCRF по умолчанию в данном режиме использует в качестве логина MAC адрес источника, а в качестве пароля - VasExperts.FastDPI). И ожидает получить в Access-Acept IP адрес, который должен совпадать с IP адресом в ARP-запросе.

```
18:0F:76:01:05:19      User-Password := "VasExperts.FastDPI"
    Framed-IP-Address = 192.168.2.199
    VasExperts-Policing-Profile = "10Mbps",
```

В файл */etc/raddb/users* также следует добавить две записи для FastPCRF

```
VasExperts.FastDPI.unknownUser Cleartext-Password := "VasExperts.FastDPI"
DEFAULT Cleartext-Password := "VasExperts.FastDPI"
```

Настройка бордера

На бордере добавляем обратный статик роут в сторону абонента (при использовании NAT на CKATe - в сторону NAT пула)

```
ip route add dst-address = 192.168.2.0 / 24 gateway = 192.168.1.2
```

Подключение тестового абонента

При подключении неизвестного абонента FastPCRF шлет Access-Request со следующим содержанием:

```
User-Name = 18:0F:76:01:05:19
User-Password =
0xC90A342D872831DFA055E3C46C89AD61D28597B3CFDB0D3B1DA3A6F4D2B8F8C9
Framed-IP-Address = 192.168.2.199
Calling-Station-Id = 18:0f:76:01:05:19
Acct-Session-Id = C702A8C000000026
Service-Type = [2] Framed
NAS-Identifier = VasExperts.FastDPI
VasExperts-Service-Type = 6
VasExperts-ARP-SourceIP = 192.168.2.199
VasExperts-ARP-TargetIP = 192.168.2.1
Message-Authenticator = 0x8FB5C8D0FAFDD71EC5F1260B695AEF7A
```

Пример Access-Accept при успешной авторизации:

```
VasExperts-User-Name = 18:0F:76:01:05:19
Framed-IP-Address = 192.168.2.199
```

```
VasExperts-Policing-Profile = 10Mbps
```

Диагностика

При внедрении L2 BRAS могут возникать различные ошибки, при которых абоненты не могут быть авторизованы и, соответственно, остаться без доступа к интернету. Ниже приведены Самые распространенные проблемы:

Нет запросов на авторизацию.

Проверить, запущен ли процесс fastpcrf. Корректно ли указан адрес Radius сервера.

Пингуется DPI, но до бордера пинг не доходит.

1. В случае использования NAT для абонентов необходим аналогичный маршрут для подсетей, используемых в NAT.

Не отправляется статистика для Accounting.

1. Проверить, разрешен ли в Firewall’е порт для приема статистики (по умолчанию 1813) на Radius сервере.
2. Проверить, подключается ли для абонента услуга 9.
3. Проверить, включен ли accounting в настройках конфигурации DPI.
4. Проверить, корректное ли значение указано для параметра netflow.

Не доходят CoA до BRAS.

Проверить, разрешен ли в Firewall’е порт для приема CoA (по умолчанию 3799) на сервере с FastPCRF.