Table of Contents

BRAS L2 ARP Example

Description

BRAS ARP L2 means that the subscriber configures the static IP address on his device. When a subscriber sends an ARP request to his default gateway, he gets to AAA in Billing. Then the subscriber is terminated by Stingray Service Gateway (SSG) and transferred to border equipment. A scheme when subscribers are given the /30 prefix is also possible.

The following elements are involved in the SSG operation scheme in BRAS L2 ARP mode:

1. Client with Q-in-Q access type
2. FastDPI - traffic processing and policing
3. FastPCRF - proxying requests between fastDPI and Radius
4. Radius server - accepts requests from fastPCRF and generates responses with specified attributes
5. Router - is responsible for packets transmission to the Internet and the backward routing. At the moment the Static Route scenario and the scenario with OSPF and BGP routing configuration on SSG are possible.

FastDPI Setup

Editing the DPI Configuration File

First, you need to uncomment (add) the following lines to the */etc/dpi/fastdpi.conf* configuration file.

```
    # enable internal database of user properties
udr=1
    # enable IP authorization mode
enable_auth = 1
    # activate L2 BRAS mode
bras_enable = 1

    # DPI "virtual" IP address (must be unique on the network)
bras_arp_ip = 192.168.1.2
    # "virtual" DPI MAC address (you should use the real MAC address of any
of the DNA interfaces)
bras_arp_mac = a0: 36: 9f: 77: 26: 58

    #IP address of the border
bras_gateway_ip = 192.168.1.1
    #MAC address of the interface to which DPI is connected on the border
bras_gateway_mac = c4: 71: 54: 4b: e7: 8a
```

```
    # data of the server where FastPCRF is installed (unless changed on the
same server as Fastdpi)
auth_servers = 127.0.0.1% lo: 29002

    # enable the response to ARP requests to gateways
bras_arp_proxy = 0x0002
    # enable authorization by ARP requests
bras_arp_auth = 2

    # vlan termination (in this case, the tag will be stripped)
bras_vlan_terminate = 1
    # local traffic closure
bras_terminate_local = 1

    # enable accounting
enable_acct = 1
    # subscriber billing statistics
netflow = 4
    # timeout for sending statistics
netflow_timeout = 60
```

You should set your **own** values for the following parameters

- bras_arp_ip
- bras_arp_mac
- bras_gateway_ip
- bras_gateway_mac

FastPCRF Setup

FastPCRF needs to be configured. To do this, edit the file */etc/dpi/fastpcrf.conf*. Find the line with RADIUS server parameters and change:

```
     # secret123 - Radius secret
     # 192.168.1.10 - IP address of the Radius server
     # eth0 - interface from which FastPCRF "communicates" with the Radius
server
     # 1812 - port to which FastPCRF sends authorization requests
     #acct_port - port to which FasPCRF sends Accounting
radius_server=secret123@192.168.1.10%eth0: 1812; acct_port = 1813
```

Radius Setup

The setting is **an example** for freeRADIUS 3 and may differ from the configuration of your Radius server.

VasExperts Dictionary

First you need to add a VSA dictionary:

- copy the dictionary /usr/share/dpi/dictionary.vasexperts from the fastpcrf distribution to the $freeRadius/share/freeradius directory
- add the following line to the main dictionary $freeRadius/share/freeradius/dictionary:

```
$INCLUDE dictionary.vasexperts
```

Creating Client Radius

Add the following lines to raddb/clients.conf of the Radius server

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

Creating a Virtual Server

To create the virtual server configuration, copy the file raddb/sites-available/default, included in the supply FreeRadius, in raddb/sites-enabled/fastdpi-vs and then edit fastdpi-vs:

- set the name of the virtual server - change the line "server default" at the beginning of the file to "server fastdpi-vs"
- in the "listen" section for auth requests (type = auth) write on which IP address and which port to listen incoming requests (note that this is the local address of the Radius server):

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

Creating a User Account

Add subscriber data to the /etc/raddb/users file. It should be noted that by default FastPCRF in this mode uses the source MAC address as the login, and VasExperts as the password. Then it expects an IP address in Access-Accept, which must match the IP address in the ARP-request.

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

Also add two entries for FastPCRF in the file */etc/raddb/users*:

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

Router Setup

On the router, add a static route to the subnet served by the DPI

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

Test Subscriber Connection

When an unknown subscriber is being connected, FastPCRF sends an Access-Request with the following content:

```
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
```

Access-Accept example on successful authorization:

```
VasExperts-User-Name = 18:0F:76:01:05:19
Framed-IP-Address = 192.168.2.199
VasExperts-Policing-Profile = 10Mbps
```

Troubleshooting

When implementing L2 BRAS/BNG, various errors may occur, so that subscribers cannot be authorized and get access to the Internet. Below are the most common problems:

No authorization requests.

Check if fastpcrf process is running. Check if the server Radius address is specified correctly.

I can ping DPI, but the ping does not reach the border.

1. In case of using NAT for subscribers, a similar route is required for the subnets used in NAT.

Statistics are not sent for Accounting.

1. Check if the port for receiving statistics is allowed in the Firewall (1813 by default) on the Radius server.
2. Check if the service 9 is activated for the subscriber.
3. Check if accounting is enabled in DPI configuration settings.
4. Check if the correct value is specified for the Netflow parameter.

CoA does not reach BRAS/BNG.

Check if the port for receiving CoA is allowed in the Firewall (3799 by default) on the server with FastPCRF.