Содержание

General BRAS setup for L2/L3 modes

FastDPI L3 BRAS setup

You need to create services and policies, which will later be transmitted using the Radius attributes from billing. An example of setting up a policy (tariff plan) and Captive Portal, which are the minimum required to start.

1. Create a file aslocal.bin (or correct this file if it already exists). The aslocal file contains those ranges of private IP addresses that are used in the provider's local network. Any of the range 64512 - 65534 is indicated for them as an autonomous system number.

```
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
```

FastPCRF authorizes only the local users. The fact whether the user is local or not is determined according to the fact of belonging his IP-address to the list of local autonomous systems.

2. Next, create the asnum.dscp file (or modify it if it already exists). The *local* numbers of autonomous system should be specified in this file, so the authorization will take place for them. Typically these are autonomous systems for the gray IP addresses specified in the aslocal.bin file, plus the white IPs allocated to the provider, if these white IP addresses are used on the local network, that is, they require authorization. Authorization will be done for all the autonomous systems IP addresses marked as local in the asnum.dscp file.

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

3. To enable authorization in **/etc/dpi/fastdpi.conf**:

```
enable_auth=1
```

4. Set the fastPCRF servers list:

```
auth_servers=127.0.0.1%lo:29002;192.168.10.5%eth1:29002
```

The format for specifying a single server: `ip%dev:port`, here `ip` is the server IP address, dev is the local device by wich the connection can be established. FastDPI connects to the first available fastpcrf server from the list.

Do not forget to activate the user property store:

```
udr=1server
```

IPv6

In order to enable IPv6 addresses authorization you should activate the IPv6 support. Actually, the Stingray SG authorizes a whole subnet with a predefined prefix length (by default it equals to /64) rather than particular individual IPv6 address. For example, if there are incoming packets sent from 2001:1::1 and 2001:1::10 addresses, only one of these addresses will be subject to authorization, so the returned authorization parameters will be applied to all the addresses from 2001:1::/64 subnet.

There is no analog of the `aslocal.bin` file for IPv6, since there are no private addresses. You must mark the AS numbers that require authorization as `local` in the `asnum.dscp` file.

IPv6 authorization is automatically enabled if fastdpi.conf has:

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

Starting from SSG version 8.1.4, it is possible to forcibly disable IPv6 address authorization by specifying in fastdpi.conf:

```
enable_auth_ipv6=0
```

Other authorization settings

Implementing of the BRAS authorization

The process of implementing a new features is always a long and thorny path especially with regard to the BRAS authorization since it requires to configure not only the fastdpi/fastpcrf but also the Radius server which handles the main part of the subscriber authorization along with the all backend data behind the Radius server which includes the data bases, billing system and so on. Below we will refer to some approaches to implement the authorization.

Test bed

Simple and reliable way to implement the BRAS authorization is to organize a test bed. Pros: it will not affect the real subscribers. Cons: it requires the additional equipment. So it is not always possible to organize a full-fledged test bed.

Separate autonomous system

As described earlier the authorization is done by using just the local IP addresses. Locality of the IP address is specified by the `local` flag for the autonomous system. Hence, one can allocate the test range of IP addresses then to set the corresponding autonomous system from the private range of

numbers(64512..65534) and to define the autonomous system as local. So the only IP addresses belonging to this local autonomous system will be authorized. "Live" subscribers will not be affected until the autonomous system with corresponding IP addresses is not defined as local. It allows you to configure the authorization on the live fastDPI.

Diagnostic IP address

So the third approach is to define that the authorization should be performed just for the specified IP addresses. For this purpose there is the `auth_trace_ip` option in the fastdpi.conf that allows you to set one or two (but not more than two) IP addresses:

```
auth_trace_ip=192.168.20.11,192.168.30.58
```

The specified IP addresses must be local (i.e. these IP addresses should be within the autonomous system declared as local, please see above). If the `auth_trace_ip` option is used so the authorization will be performed just for the IP addresses specified therein.

Authorization settings

You can specify the following authorization options in fastdpi.conf in addition to described earlier:

`auth_resend_timeout` - is the timeout of authorization requests resending to the fastpcrf, in seconds. The default value is 60. If the fastDPI doesn't receive a response from the fastpcrf during this period, the authorization request will be repeated.

`auth_expired_timeout` - is the authorization lifetime, in minutes. The default value is 60 minutes. Zero value corresponds to unlimited authorization lifetime. This option is applied only in case the Radius response does not contain the `Session-Timeout` attribute specifing the session lifetime. Note that the Access-Reject also can contain the `Session-Timeout` attribute. Once that time has elapsed, a second authorization request is sent.


`auth_expired_timeout=0` (unlimited authorization lifetime) may result in subscriber being rejected in authorization (Access-Reject) will remain in "unauthorized" state permanently. The subscriber "unauthorized" state can be altered just by CoA notification to reauthorization, by the fastDPI restart or manually using the fdpi_ctrl.

`auth_pcrf_reconnect` - the timeout of reconnect to the fastpcrf, in seconds. The default value is 1 second.

Diagnostic settings

`auth_trace` - is the boolean flag enabling the authorization tracing, is not specified by default. Note that the authorization tracing significantly affects the performance of the fastDPI and causes the large number records being written to the logs, so it should not be enabled unless you have to.

`auth_trace_ip` - the list of IP addresses (no more than two) to be authorized. The list is empty by

default. Example:

```
auth_trace_ip=192.168.10.20,192.168.30.45
```

This list can be applied at the authorization implementing stage and when configuring the Radius servers: the authorization will only be performed for the specified local IP addresses (typically testing subscribers are used) without affecting "real" subscribers.

FastDPI L2 BRAS setup

The activation of the fastDPI BRAS features is done according to **the mandatory settings** defined in the **fastdpi.conf** configuration file:

- `bras_enable=1` – the common flag to enable the BRAS
- `bras_arp_ip` – specifies the BRAS IPv4 address. You are allowed to set a fake IP addres, which is not connected to any network interface. The main requirement is that the IP address should be unique, i.e. it should not correspond to any user.
- `bras_arp_mac` – the BRAS MAC address in the following format: XX:XX:XX:XX:XX:XX, for example, a0:00:b1:01:4e:cc. This MAC address have to be unique within the whole local network; fake MAC can be used instead, it should not be connected to any network card, but in order to avoid an accidental match with other MAC address of client's equipment we strongly recommend to use the real dna card MAC address instead.
- `auth_servers` - specifies the list of the fastPCRF servers. FastPCRF server is responsible for interaction with Radius servers. Used format to specify the server: `ip%dev:port`, here ip - is the server IP address, dev - the local device used to establish connection. FastDPI establishes connection with the first available fastPCRF server from the list.

In order the fastDPI BRAS to work properly BRAS have to be enabled UDR (user data repository is the internal database containing user properties): the **fastdpi.conf** should contain the following line

```
udr=1
```

Example:

```
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
```

When choosing the `bras_arp_mac` parameter, it is very convenient to use the existing MAC address of the card port. But it was noticed that some advanced cards (for example, 25G cards on the XXV710 chip, i40e driver) can destroy some packets (for example, ARP) if `bras_arp_mac` is equal to the MAC address of the card port. The reason for this behavior is not clear, therefore, in order to avoid packet loss, we advise

you to select the `bras_arp_mac` value purely virtual, not matching the MAC address of the port.

Some special fastDPI BRAS features are enabled by corresponding advanced settings described further, but without the `bras_enable=1` flag the special features will be unavailable.

IPv6 Setup

L2 BRAS (BNG) supports allocating of stateful DHCPv6 IPv6 addresses. In this mode, IPv6-address is allocated to the subscriber with DHCPv6. Automated allocation of IPv6-addresses (SLAAC/stateless DHCPv6) is not supported.

The concept of the work scheme looks like this:

1. subscriber's CPE searches for the IPv6-router using ICMPv6. DPI announces itself as an IPv6-router. It specifies that DHCPv6 is needed in order to receive an IPv6-address;
2. CPE sends a DHCPv6-request to obtain an IPv6-address;
3. DPI intercepts all DHCPv6 subscriber requests and processes them, in fact it is acting as a DHCPv6 server. If the DPI has no information on such subscriber or the session has expired, DHCPv6-request is transferred to Radius with PCRF;
4. PCRF receives a response from Radius. Among other parameters, it contains subscriber's IPv6-prefix and PD-prefix (prefix delegation) if needed. Then the response is transferred back to DPI;
5. Having the data from PCRF, DPI sends a DHCPv6-response to the subscriber. DPI allocates one IPv6 address from the IPv6 prefix given to the subscriber, while the PD-prefix is transmitted to the subscriber completely. Despite that only one address is allocated from an IPv6-prefix, all IPv6 addresses of this prefix belong to this subscriber. Actually, the subscriber can request several IPv6-addresses, – they will all be issued from the IPv6 prefix provided.

It should be specially noted that the Radius should allocate a fixed-length IPv6 prefix to the subscriber. Prefix length is set by parameter ipv6_subnetwork, /64 is the default value. PD-prefix length also has to be equal `ipv6_subnetwork`.

If the subscriber has both IPv6- and PD-prefix, then such subscriber must be marked as multi-bind. The reason is that such subscriber holds ***two*** IPv6-prefixes; Radius response should contain attribute `VasExperts-Multi-IP-User=1`.

Enabling IPv6 BRAS/BNG

IPv6 BRAS/BNG mode is enabled automatically, if there is a setting in *fastdpi.conf*

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

You can disable IPv6 BRAS by setting in *fastdpi.conf*:

```
bras_ipv6=0
```

The bras_ipv6 parameter can be turned off (`bras_ipv6=0`) without DPI restart.

DHCPv6 request processing mode is enabled since IPv6 BRAS is enabled. You can disable DHCPv6 and ICMPv6 Router Solicitation by setting in *fastdpi.conf*

```
bras_dhcp6_mode=0
```

Additionally you can set the following parameters in *fastdpi.conf*:

- `bras_ipv6_link_local` - link-local DPI address (from FE80::/10). If this parameter is not set, link-local address is computed automatically from bras_arp_mac. DPI always has a link-local address.
- `bras_ipv6_address` - sets the global DPI IPv6-address. For example, the global address can be useful for pinging DPI from the subscriber. If this parameter is not set, DPI does not have a global IPv6-address.
- ICMPv6 Options
- DHCPv6 Options

Radius-Server Intergation

Example of an Access-Request for allocating IPv6 prefixes to the subscriber:

```
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
```

In this example, QinQ is a subscriber's ID, request is initiated by Solicit DHCPv6 packet (`VasExperts-Service-Type = DHCPv6`, `VasExperts-DHCPv6-Request = Solicit`), the subscriber request includes PD-prefix (`VasExperts-DHCPv6-Delegated = 1`).

CPE can request an IPv6-address and a PD-prefix either in one or separate DHCPv6-requests. That is why you should not rely on the `VasExperts-DHCPv6-Delegated` attribute value: even if the subscriber does not request a PD-prefix, the Radius can allocate one. The DPI will save it, and if the CPE will request it later, DPI will return the

previously allocated PD

Example of response:

```
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:de1e: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"
```

In this example, the subscriber recieves two **different** prefixes:

- `Framed-IPv6-Prefix = 2001:cafe:32:106::/64` - DPI will allocate IPv6 addresses to a subscriber from this pool
- `Delegated-IPv6-Prefix = 2001:de1e:32:106::/64` - this delegated prefix is transmitted to CPE (if the CPE requests PD)

It is important to note:

1. for IPv6, the address **always** has to be bound with login. Login is a unique subscriber ID, which can be associated with many IPv4-addresses and IPv6-prefixes. Subscriber's login is specified in `Access-Accept` in attribute `User-Name` or `VasExperts-UserName`.
2. If the subscriber has several IPv6-prefixes (like in the example given - IPv6-prefix and PD-prefix), then such subscriber must be marked as multi-bind (`VasExperts-Multi-IP-User = 1` attribute).

`Session-Timeout` attribute sets the time for DPI session (same as accounting-session time): during this time all DHCPv6-requests from this client will be processed by DPI, using parameters previously issued by the Radius. After `Session-Timeout` seconds, the current accounting-session will be closed and DHCPv6-request will be transferred again in Radius Радиус Access-Request. If there is no `Session-Timeout` attribute in Radius responce, it is considered to be equal with fastdpi.conf-parameter auth_expired_timeout.

IPv6 prefix leasing time is set by fastdpi.conf-parameters bras_dhcp6_preferred_lifetime and bras_dhcp6_valid_lifetime. You can set the leasing time individually for each subscriber using the Radius attribute `DHCP-IP-Address-Lease-Time`: this attribute sets preferred lifetime; valid lifetime is twice as big.

Additional DHCPv6-options can be set with special VasExperts VSA attributes.

Setting DHCPv6-options in Radius

Stingray SG supports setting practically any DHCPv6 option via special VasExperts VSA attributes. If Stingray SG was installed using standard tools from the official VasExperts repository, then the updated dictionary of all VSA VasExperts is located in the /usr/share/dpi/dictionary.vasexperts file. All of these attributes are strings with the same format:

```
opt:value
```

here:

- `opt` - number, option ID, `value` - option value.

VSA attribute	Description
VasExperts-DHCP-Option-IPv6	Options specifying an IPv6-address or a list of IPv6-addresses
VasExperts-DHCP-Option-IPv6-Prefix	Options specifying IPv6-prefix
VasExperts-DHCP6-Option-Num	Specifies an option with a numeric value
VasExperts-DHCP6-Option-String	Specifies an option with a string value
VasExperts-DHCP6-Option-Bin	Specifies a binary option as a hex string. Note that when setting a binary option, its value must be in the network byte orderc

Example (FreeRadius format):

```
  # Option 22 - list of IPv6 addresses of SIP servers:
  # Stingray SG will send one option 22 to DHCPv6 with the value - a list of
specified IPv6 addresses
&VasExperts-DHCP-Option-IPv6 := "22:2c0f:ff91::10:1"
&VasExperts-DHCP-Option-IPv6 += "22:2c0f:ff91::10:2"
  # Option 71 - MIPv6 Home Network Prefix Option
  # sets IPv6-prefix
&VasExperts-DHCP-Option-IPv6-Prefix += "71:2c0f:ff90:71::/56"

  # Option 32 - OPTION_INFORMATION_REFRESH_TIME, numeric:
&VasExperts-DHCP6-Option-Num  += "32:55779"

  # Option 27: NIS-server IPv6-address, specified in binary
&VasExperts-DHCP6-Option-Bin  += "27:2c0fff91000000000000000000200001"
  # the same can be set another way:
  # &VasExperts-DHCP-Option-IPv6 += "27:2c0f:ff91::20:1

  # Option 43: ERO (Relay Agent Echo Request option)
  # given as an example of setting an option with a value list of numbers
  # Stingray SG will combine all attributes of 43 options into one DHCPv6
option with the value '50,60,32'
&VasExperts-DHCP6-Option-Num  += "43:50"
&VasExperts-DHCP6-Option-Num  += "43:60"
  # int16-option in binary form (value 32)
&VasExperts-DHCP6-Option-Bin  += "43:0020"
```

A complete up-to-date list of all DCHPv6 options and RFC references can be found at the IANA web-

site.

ICMPv6 settings for fastDPI

The following ICMPv6 Router Solicication/Advertisement processing parameters can be set in fastdpi.conf; most of these parameters are defined in RFC 4861:

Parameter	Format	Default Value	Description
bras_ipv6_router_pref	number	0	BNG mode and priorities as IPv6 router: **-1** - BNG is not an IPv6 router, it does not process ICMPv6 Router Solicitation and does not send Router Advertisement; **0** - BNG is an IPv6 router with Medium priority; **1** - BNG is an IPv6 router with High priority; **3** - BNG is an IPv6 router with Low priority
bras_icmp6_rtradv_mtu	number	1500	The MTU specified in the Router Advertisement. Value 0 - do not add MTU option to Router Advertisement
bras_icmp6_reachable_time	number	0	*AdvRetransTimer*, milliseconds. Used by IPv6 clients - the time between retransmission of Neighbor Solicitation messages. **0** - not set by the router
bras_icmp6_hop_limit	number	64	*AdvCurHopLimit* the value of the Hop Limit field of IPv6 packets
bras_icmp6_default_lifetime	number	1800	*AdvDefaultLifetime*, seconds. Used by IPv6 clients to build a list of default routers. A 0 value indicates that BNG is not the default router.

Unsolicited RA

Since Stingray SG in L2 BNG mode is an IPv6 router, according to RFC 4861 it periodically announces itself to the local network with ICMPv6 Router Advertisement (unsolicited RA) message.

Parameter	Format	Default value	Description
bras_icmp6_send_rtradv	number	0	Send (1) or not (0) the periodic RA
bras_icmp6_min_rtradv_interval	number	200	Initial boundary of periodic RA sending interval, seconds
bras_icmp6_max_rtradv_interval	number	600	Ending boundary of periodic RA sending interval, seconds

When the unsolicited RA sending mode is enabled, the time of the next RA sending is randomly selected from the interval [`bras_icmp6_min_rtradv_interval`, `bras_icmp6_max_rtradv_interval`] for each active DHCPv6 subscriber.

DHCPv6 settings for fastDPI

The following DHCPv6 processing parameters can be set in fastdpi.conf:

Parameter	Format	Default value	Description
bras_dhcp6_enable_rapid_commit	number	0	Rapid Commit enabled or disabled The usual procedure for issuing an address in DHCPv6 consists of 4 steps (2 requests + 2 responses). You can use a 2-step procedure (Rapid Commit): **0** - disable Rapid Commit; **1** - enable Rapid Commit. The 2-step procedure for issuing an address will only apply to clients with Rapid Commit support
bras_dhcp6_enable_unicast	number	0	Server Unicast enabled or disabled **0** - unicast disabled. DHCPv6 unicast-requests from the client side will be ignored. **1** - unicast enabled.
bras_dhcp6_preferred_lifetime	number	3600	Preferred IPv6 lease time, seconds. This value must be less than `bras_dhcp6_valid_lifetime`
bras_dhcp6_valid_lifetime	number	7200	IPv6 lease time, seconds. This value must be more than `bras_dhcp6_preferred_lifetime`.
bras_dhcp6_preference	number	-1	The value of the Preference option in the DHCPv6 Advertise. This option sets the preference for a DHCPv6 server in a network with multiple DHCPv6 servers. **-1** - does not specify the Preference option in the DHCPv6 Advertise.
bras_dhcp6_nak_lifetime	number	60	[Stingray SG 8.3] Lifetime of the Radius Reject response, seconds If Radius has not issued an IPv6 address to the client, the client can retry frequent DHCPv6 requests, causing a storm of Access-Request for Radius. With this parameter, you can set the period of time during which the Stingray SG itself will respond to requests from such clients.