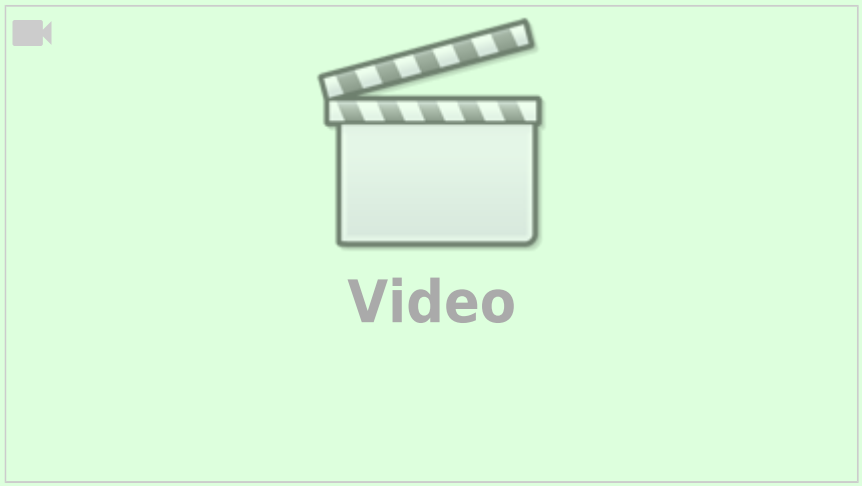
Содержание

PPPoE Authorization Setup

L2 PPPoE Mode Overview:



FastDPI BRAS supports PPPoE since 7.2 version. In order to enable the PPPoE support it is needed to:

1. activate the BRAS
2. set in the fastdpi.conf file a number of settings:

```
    # Enable PPPoE
bras_pppoe_enable=1
    # Specify maximum number of PPPoE-sessions
    # its recommended value should be 1.5 or 2 times higher than the number
of PPPoE subscribers
bras_pppoe_session=10000

    # IP and MAC addresses of a gateway placed behind the SSG must be
properly configured
    # (subscriber -> SSG -> gateway)
bras_gateway_ip=192.168.0.1
bras_gateway_mac=aa:bb:cc:dd:ee:ff
```

PAP, CHAP and MS-CHAPv2 authentication protocols are supported. The list of permitted authentication protocols is set by conf-option `bras_ppp_auth_list`. The protocols in the list are arranged in order of preference, so the first one is the most preferred. Identifiers of supported protocols:

- 1 - PAP is deprecated
- 2 - CHAP-MD5
- 3 - MS-CHAPv2

All the mentioned abobe protocols, except the first one (PAP), are permitted by default:

```
bras_ppp_auth_list=2,3
```

MAC address authentication is also allowed if the following setting is set in fastdpi.conf:

```
bras_ppp_mac_auth=1
```

MAC address authentication is used in case the negotiation of authentication protocol is failed.

- Additional PPPoE BRAS settings
- PPPoE-sessions authentication the Radius server

ARP handling in PPPoE

ARP-requests coming from the subscriber do not make sense in PPPoE-networks, since PPPoE is a point-to-point connection and the subscriber are allowed to send packets only to a PPPoE server which MAC address is known to the subscriber.

All ARP-requests in the format "Who is IP=x.x.x.x?", here x.x.x.x is the IP address of "alive" PPPoE subscriber coming from the the WAN are handled by SSG. SSG returns the `bras_arp_mac` option value in response. That is, SSG replies to ARP requests to the current PPPoE sessions.

If NAT-service is assigned to a PPPoE-subscriber, WAN ARP-requests to PPPoE sessions are not processed.

All the main functions of BRAS are supported for PPPoE sessions:

- IP source guard
- Local traffic locking, including heterogeneous traffic, like when one segment is PPPoE network and another is the DHCP-network.

PPPoE sessions recovery after DPI restart

At start, fastDPI tries to restore subscribers PPPoE sessions from UDR so that short-term service restart is seamless for subscribers. In some billing systems such restoration can lead to mismatching of sessions state in the DPI and the billing, especially if IP addresses are asiigned dynamically: when assigning addresses the billing sysrem might follow the sequence Access-Request + Acct-Start, while there is only Acct-Start during session restore.

In fastDPI 8.3, it became possible to disable the restoration of subscribers PPPoE sessions during the restart: use `bras_pppoe_restore_on_startup` fastdpi.conf parameter.

```
# To restore PPPoE-sessions at fastDPI start
    # 1 (default) - to restore
    # 0 - not to restore. New subscriber sessions will be created.
#bras_pppoe_restore_on_startup=1
```

You should specify `bras_pppoe_restore_on_startup=0` in fastdpi.conf in order to disable PPPoE sessions recovery. Then the subscriber will have to create a new PPPoE session and to repeat

authorization. If the subscriber tries to access to the previous session, then Stingray Service Gateway will send a PADT-packet in session termination.

Configuring Service-Name for VLAN

Service-Name is available starting from SSG version 12.3!

The Service-Name tag is required to set the authorization procedure according to RFC requirements. The SSG fully supports this tag according to all requirements.

The tag indicates that the service name follows. The TAG_VALUE field is a UTF-8 character string with no terminating NULL character. The zero value of the TAG_LENGTH field is used to indicate the acceptability of any service. An example of using the Service-Name tag is to indicate ISP2 name, class, or quality of service.

It is managed separately for each VLAN ID.

You can access a quick guide to Service-Name management with the command

```
fdpi_cli help vlan group
```

Output of group properties

Output all properties for all groups:

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

Output all properties for a group with a specific ID:

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

Here ID is the VLAN number for which you want to output Service-Name information.

Example:

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

Show PPPoE authorization policy:

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

Show all protocols authorization policy:

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

Show the policy for using service names for authorization using PPPoE:

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

Authorization permission

Enable authorization via PPPoE on a specific VLAN:

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

Allow authorization via PPPoE for a specific Service-Name:

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

When establishing a PPPoE session in the Discovery stage after receiving a PADI packet, a time delay (parameter `delay`) is allowed before sending the PADO packet. The allowed values of the `delay` parameter are: 0, 1, 2, 3, 4, 5.

Allow authorization via PPPoE for a specific Service-Name with a delay (measured in seconds):

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

Example:

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

Authorization denial

To deny authorization for a specific VLAN, you must first remove all existing rules for that VLAN. That is, to allow specific Service-Names, you must first disallow all of them and only then allow specific tags.

Deny authorization through PPPoE on a specific VLAN:

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

Deny authorization via PPPoE for a specific Service-Name:

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

Example: Allow authorization only for a specific 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
```

Example: Deny authorization only to a specific 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'
```

When introducing rules, the sequence of commands is important. For example, if you enter a general authorization prohibition after the enabling rules, authorization with any Service-Name in vlan 1250 will not be available:

```
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
```

This restriction also applies to single prohibitions/permissions.

Example: allow authorization with 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'
```

Example: Deny authorization with 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'
```

Other commands

Delete Service-Name and its properties:

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

Packet drop without analysis:

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

Packet pass without analysis:

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

Delete all rules for all started VLANs (equivalent to processing the default VLAN):

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