Table of Contents

PPoE Radius Access-Request	. 3
1. Access-Request Format	. 3
Support for PPPoE options circuit-id and remote-id	
Support for Huawei vendor-specific tag 1	
2. Access-Accept Format	
Session Lifetime	
3. Access-Reject Format	. 6
Why is Access-Reject needed for "our" subscribers?	

PPPoE Radius Access-Request

PPPoE sessions authorization is performed by the Radius server through the fastPCRF server, see the fastPCRF settings. FastPCRF is the part of the Stingray SG and is essentially a proxy between the fastDPI and a third-party Radius server.

Access-Request requests and Access-Accept along with Access-Reject responses differ from those used in L3-authorization.

1. Access-Request Format

The Access-Request generated by fastPCRF contains the following Radius attributes:

- User-Name for PAP/CHAP/MS-CHAPv2: subscriber login. For MAC address authorization, this
 attribute contains the subscriber's MAC address as a string, similar to the Calling-Station-Id
 attribute
- Password subscriber password (only for PAP authorization)
- CHAP-Challenge and CHAPPassword- for CHAP authorization
- MS_CHAP_Challenge and MS_CHAP2_Response (Microsoft VSA) for MS-CHAPv2 authorization
- Calling-Station-Id subscriber's MAC address as a string, e.g., '01:02:e4:55:da:f5'. Lowercase letters are used for hex digits A-F
- Acct-Session-Id accounting session identifier. This attribute is always sent, even if you do not use SSG's accounting.
- Service-Type = 2 (Framed)
- Framed-Protocol = 1 (PPP)

[SSG 7.6+] If the Access-Request is initiated by a CoA reauthorization request, then the Framed-IP-Address attribute is also added, containing the IP address assigned to this subscriber.

Attributes identifying the NAS (i.e., SSG):

NAS-IP-Address, NAS-Identifier - IP address or identifier of the fastdpi server, set in the fdpi_server parameter. Note that by default, only one of the attributes - NAS-IP-Address or NAS-Identifier - is added to the Access-Request, depending on the fdpi_server settings, with attr_nas_ip having priority. The radius_add_all_nas_ids parameter allows adding both of these attributes to the request:

```
# Allows adding both NAS-IP-Address AND NAS-Identifier attributes
```

- # According to RFC, a request can contain either NAS-IP-Address or NAS-Identifier.
- # If values for both options are set, priority is given to the NAS-IP-Address option.
- # Setting this parameter to 1 allows adding both attributes to the request.

#radius add all nas ids=0

VASExperts-Service-Type - Vendor-Specific attribute, contains a number (int32) defining the

PPPoE authorization type:

- VASExperts-Service-Type = 2 for PAP
- VASExperts-Service-Type = 3 for CHAP
- VASExperts-Service-Type = 4 for MS-CHAPv2
- VASExperts-Service-Type = 5 for MAC address authorization

Message-Authenticator - [RFC2869] generated if in **fastpcrf.conf** the parameter radius msg auth attr=1

If the subscriber's incoming packet contains VLAN (i.e., if you have a PPPoE network with L2 VLAN tags):

- NAS-Port-Type configured in **fastpcrf.conf**, parameter radius_attr_nas_port_type, default value 5 (Virtual)
- NAS-Port VLAN value

If the subscriber's incoming packet contains QinQ (i.e., if you have a PPPoE network with L2 QinQ tags):

- NAS-Port-Type configured in **fastpcrf.conf**, parameter radius_attr_nas_port_type, default value 5 (Virtual)
- NAS-Port-Id VLAN value as a string in the format "outerVLAN/innerVLAN", e.g., "10/102"

Support for PPPoE options circuit-id and remote-id

SSG starting from version 8.2 supports PPPoE options circuit-id and remote-id according to RFC 4679. The values of these options are transmitted in the Access-Request in VSA attributes Agent - Circuit-Id and Agent-Remote-Id respectively, vendor-id=3561.

Support for Huawei vendor-specific tag 1

SSG 12.4 — added support for Huawei vendor-specific tag 1.

The value is interpreted as ADSL-Forum-Circuit-Id.

If a PPPoE packet contains both Circuit-Id and Huawei tag 1, preference is given to Circuit-Id, and Huawei tag 1 is ignored.

2. Access-Accept Format

An Access-Accept response means the subscriber is authorized, has sufficient balance, and has been assigned an IP address. Dual stack is supported: both IPv4 address and subscriber properties, as well as IPv6 address, including PD prefix, can be specified in one response.



SSG 8.4 implemented support for the Framed-Pool attribute: in the response, instead of Framed-IP-Address, the name of the pool from which the subscriber's IP address



should be allocated can be specified, for more details see Локальный DHCP (Пулы IPадресов). Framed-IP-Address in the following description should be read as it can be obtained from a pool, not explicitly specified in the Radius response

Attributes:

- Framed-IP-Address mandatory attribute: IP address assigned to the subscriber.
- Idle-Timeout optional attribute: inactivity timeout, in seconds. The PPPoE session will be closed if there are no packets from/to the subscriber during this time. If this attribute is not set, the value of the bras ppp idle timeout parameter from fastdpi.conf is used
- Reply-Message optional attribute: message that will be transmitted to the subscriber in the PPP Auth-Ack response
- Session-Timeout optional attribute: max session lifetime, seconds.
- Acct-Interim-Interval optional attribute: interval for sending interim accounting data, seconds (cannot be less than 60). 0 do not send interim accounting.
 - Explicitly setting Acct-Interim-Interval = 0 in the RADIUS response disables sending Interim-Update.
- Class optional attribute: this attribute, if set, will be sent "as is" in all accounting packets
- MS-CHAP2-Success Microsoft VSA attribute [RFC2548], mandatory for MS-CHAPv2 authorization

The following Microsoft VSA attributes are supported (vendor-id=311, RFC2548), all are optional:

- MS-Primary-DNS-Server IP address of the primary DNS server
- MS-Secondary-DNS-Server IP address of the secondary DNS server
- MS-Primary-NBNS-Server IP address of the primary NetBios server
- MS-Secondary-NBNS-Server IP address of the secondary NetBios server

VASExperts VSA attributes (vendor-id=43823), are optional:

[41] VASExperts-DHCP-DNS - IP address of the DNS server. There can be no more than two VASExperts-DHCP-DNS attributes: for primary and secondary server.

DNS server addresses can be set via Microsoft VSA attributes or VASExperts VSA attribute.

IPv6 support: both IPv4 and IPv6 attributes must be returned in one Access-Accept response. Supported IPv6 attributes:

- 1. Framed-IPv6-Prefix IPv6 prefix assigned to the subscriber. The prefix length must be equal to ipv6 subnetwork
- 2. Framed-IPv6-Address subscriber's IPv6 address. SSG converts this address to a prefix using the ipv6 subnetwork parameter
- 3. Delegated-IPv6-Prefix PD prefix assigned to the subscriber. The prefix length must be equal to ipv6 subnetwork
- 4. DNS-Server-IPv6-Address IPv6 address of the DNS server. There can be several of these attributes one for each DNS server.
- 5. Framed-IPv6-Pool
- 6. Framed-IPv6-Route.
- 7. VSA attributes for DHCPv6 options

In addition to the above attributes, Access-Accept must contain the subscriber's policing profile and list of connected services, see subscriber property attributes

Session Lifetime

If the Session-Timeout attribute is not present in the response, then the PPPoE session is considered permanent and ends either by explicit disconnect from the subscriber or by inactivity timeout.

If Session-Timeout is specified, then SSG will terminate the PPPoE session after this time has elapsed. Termination of the PPPoE session is clearly described in the PPP/PPPoE specifications and involves sending special term messages to the subscriber; the subscriber, upon receiving term, can create a new PPPoE session.

3. Access-Reject Format

There are two possible types of subscriber "unauthorized" status:

- the subscriber is ours, but for some reason (zero balance, blocked, etc.) they cannot be granted the full range of services
- the subscriber is unknown to us in this case, the subscriber should not be allowed into the network

In the first case (our subscriber), the subscriber needs to be assigned an IP address (i.e., the PPPoE session will be established, authorization successful), but reduced settings should be applied - a special policing profile, service 5 (whitelist + captive portal) - so that the subscriber can access the network and, for example, top up their balance. That is, Access-Reject should contain the Framed-IP-Address attribute for such subscribers.

In the second case (unauthorized subscriber, error in authorization parameters), the Access-Reject packet should not contain the Framed-IP-Address attribute, which is interpreted as a network access ban: the PPPoE session is not established, authorization fails.

Access-Reject contains the following attributes:

- Framed-IP-Address IP address assigned to the subscriber. If the subscriber is "unauthorized", they should not be assigned an IP address, meaning the Framed-IP-Address attribute should not be present in Access-Reject.
- Idle-Timeout inactivity timeout, in seconds. The PPPoE session will be closed if there are no packets from/to the subscriber during this time. If this attribute is not set, the session is considered permanent (until explicitly closed by the subscriber)
- Reply-Message optional attribute: message that will be transmitted to the subscriber in the PPP Auth-Ack/Auth-Nak response
- Session-Timeout optional attribute: max session lifetime, seconds.
- Acct-Interim-Interval optional attribute: interval for sending interim accounting data, seconds (cannot be less than 60). 0 do not send interim accounting.
 - Explicitly setting Acct-Interim-Interval = 0 in the RADIUS response disables sending Interim-Update.
- Class optional attribute: this attribute, if set, will be sent "as is" in all accounting packets

For MS-CHAPv2 authorization type, the MS-CHAP-Error [RFC2548] attribute is also supported.

The following Microsoft VSA attributes are supported (vendor-id=311, RFC2548), all are optional:

- MS-Primary-DNS-Server IP address of the primary DNS server
- MS-Secondary-DNS-Server IP address of the secondary DNS server
- MS-Primary-NBNS-Server IP address of the primary NetBios server
- MS-Secondary-NBNS-Server IP address of the secondary NetBios server

VASExperts VSA attributes (vendor-id=43823), are optional:

[41] VASExperts-DHCP-DNS - IP address of the DNS server. There can be no more than two VASExperts-DHCP-DNS attributes: for primary and secondary server.

DNS server addresses can be set via Microsoft VSA attributes or VASExperts VSA attribute.

If the subscriber is authorized, i.e., they have been assigned an IP address, then in addition to the above attributes it is **mandatory** to set the policing profile VasExperts-Policing-Profile and service profile 5 (whitelist + Captive Portal) VasExperts-Service-Profile in special VASExperts VSA attributes, for more details see L3 BRAS.

Why is Access-Reject needed for "our" subscribers?...

The policing profile and services set in Access-Reject are applied temporarily. If the subscriber properties received in the Access-Accept attributes are stored in the internal database (UDR) of fastDPI and are applied even after a reboot, then the properties from Access-Reject are applied without saving to UDR. That is, upon reboot of fastDPI, the subscriber properties that came last in Access-Accept will be restored, and fastDPI will apply them until it receives new ones in response to an Access-Request.