Содержание

Access-Reject format for PPPoE networks

There are two types of "unauthorized" subscriber:

- the subscriber is our, but he can not be delivered a full range of services for some reason (zero balance, he is blocked, etc.),
- the subscriber is not known to us - in this case the subscriber can not be allowed to access the network

In the first case (the subscriber is our), the subscriber have to be assigned an IP address (i.e. the PPPoE session will be established, the authorization is successful), but the restricted settings - the special policing profile, service 5 (whitelist + captive portal) - should be set to provide the user access to the network, for example, to top up his balance. That is, Access-Reject must contain the Framed-IP-Address attribute for such subscribers.

In the second case (the subscriber is not known to us, there is an error in the authorization parameters), the Access-Reject package must not contain the Framed-IP-Address attribute - it is treated as the network access is forbidden: the PPPoE session will not be set and the authorization will be failed.

Access-Reject contains the following attributes:

- `Framed-IP-Address` - the IP address assigned to the subscriber. If subscriber is "undesirable", he haven't to be assigned an IP address, that is, the Access-Reject should not contain the Framed-IP-Address attribute.
- `Idle-Timeout` - the inactivity timeout, in seconds. The PPPoE session will be closed if there were no packets from/to the subscriber during the timeout. If this attribute is not specified, the session is considered to be unlimited (until it is explicitly terminated by the subscriber)
- `Reply-Message` - optional attribute: the message to be sent to the subscriber in the Auth-Ack/Auth-Nak PPP response
- `Session-Timeout` - optional attribute: maximum session lifetime, in seconds.
- `Acct-Interim-Interval` - optional attribute: the period of sending the accounting intermediate data, in seconds (can not be less than 60). 0 - do not send intermediate accounting.
- `Class` - optional attribute: if this attribute is specified, it will be sent "as is" in all accounting packages

The `MS-CHAP-Error` [RFC2548] attribute is also supported for the MS-CHAPv2 authorization type.

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

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

The VAS Experts VSA attributes (vendor-id = 43823) are optional:

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

DNS server IP addresses can be specified through the Microsoft VSA attributes or VAS Experts VSA-attribute.

If the subscriber is authorized, i.e., he is assigned an IP address, then in addition to the above-mentioned attributes **it is necessary** to specify the `VasExperts-Policing-Profile` policing profile and the `VasExperts-Service-Profile` service profile 5 (whitelist + Captive Portal) within the special VAS Experts VSA attributes, for more details see L3 BRAS.

Why do we need "Access-Reject" for our subscribers? ..

The policing profile and services specified in the Access-Reject are applied temporarily. The subscriber properties being received in the Access-Accept attributes are stored in the internal fastDB (UDR) database and are applied even after rebooting, whereas the properties being received in Access-Reject are applied without saving in the UDR. That is, when the fastDPI is rebooted, the subscriber properties being received last time in the Access-Accept will be restored and the fastDPI will apply them until the new ones will be received in response to the Access-Request.