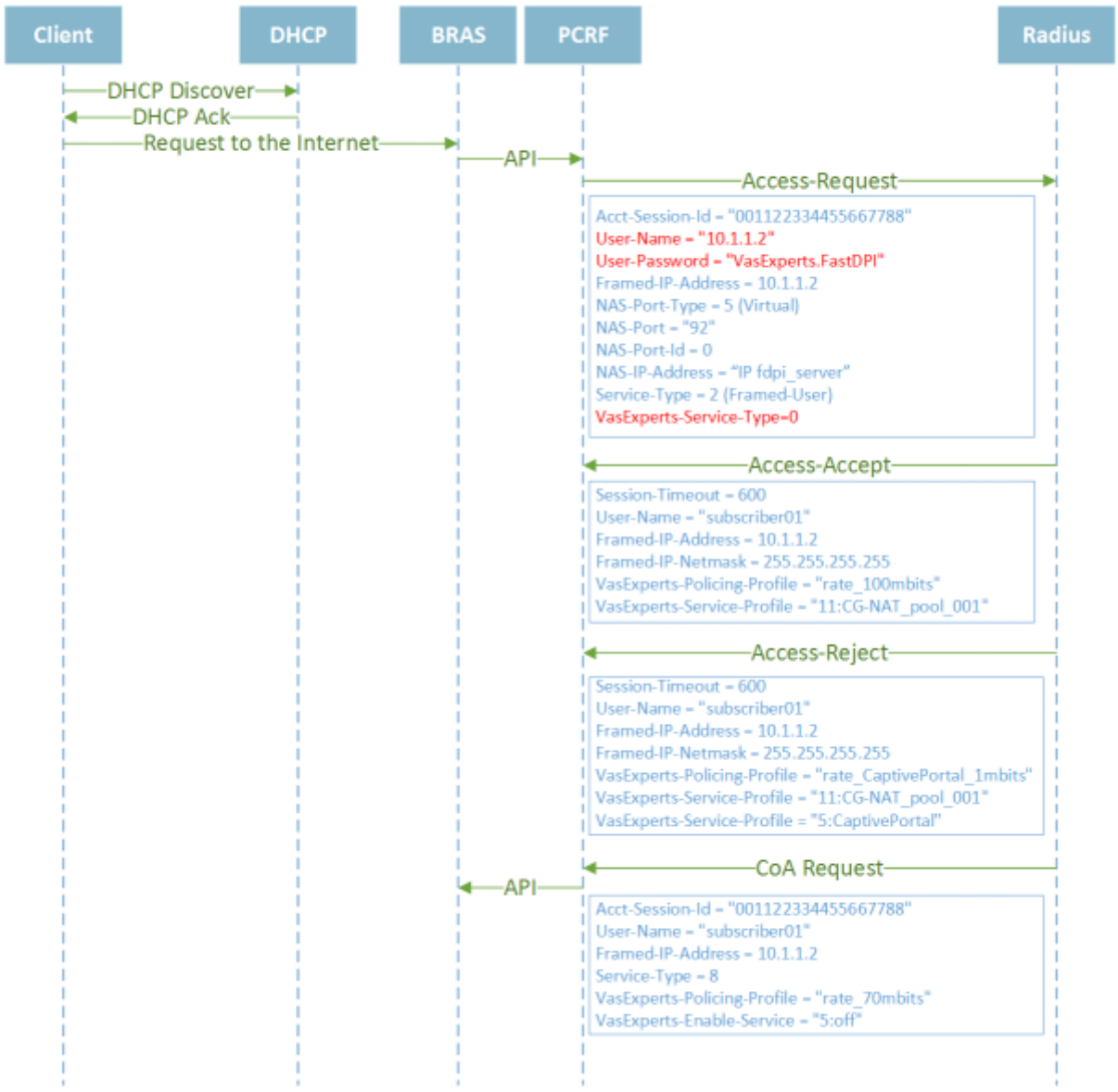
Table of Contents

Process of AAA authorization for L3 IPoE subscriber sessions

Description

The fastPCRF server actually acts as an authentication server (L3 BRAS) for the fastDPI: for outgoing client traffic fastPCRF requests the Radius server for the client authentication, policing profile (analogue of the tariff plan) and service profiles. CoA (Change of Authorization) alerts are also supported - notification of the Radius server about changes in the user settings (balance exhaustion, policing changes, etc.)



When you start the Stingray Service Gateway (SSG), the authorization state of all the users is set to "unknown". Previously stored in the fastDPI internal base (UDR) user settings are applied according to this state. When an outgoing packet is received from a local IP address, the SSG analyzes the authorization state and if it is unknown the SSG sends an authorization request to the fastPCRF

server. Essentially, this is an Access-Request Radius request.
When the Radius server reply is received, the fastPCRF sends user properties to the fastDPI, which in turn set the authorization status either to **"authorized" (Accept-Accept)** or **"unauthorized" (Accept-Reject) state**.

If a subscriber resides in "unauthorized" state, the Stingray Service Gateway itself doesn't limit subscriber's traffic. In order to limit traffic the special parameters should be received within the Access-Reject, they are the following: special policing (highly truncated bandwidth) and service 5 (Allow list) specifying the sites an unauthorized user is allowed to access - usually it is the captive portal.