

RFC 6911 : RADIUS attributes for IPv6 Access Networks

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 avril 2013

Date de publication du RFC : Avril 2013

<http://www.bortzmeyer.org/6911.html>

Le protocole RADIUS joue un rôle important dans l'accès à l'Internet : c'est le principal mécanisme utilisé pour faire communiquer la machine qui contrôle l'accès physique avec la machine qui contient la base des utilisateurs et les informations sur les autorisations, les configurations spécifiques... RADIUS avait bien sûr déjà la capacité de transporter des informations IPv6 mais ce nouveau RFC en ajoute quelques unes.

Une petite révision sur RADIUS d'abord (vous pouvez suivre sur la figure 1 du RFC). Lorsqu'un utilisateur accède à l'Internet, plusieurs machines sont utilisées. Il y a d'abord la machine terminale de l'utilisateur, ou bien un petit routeur, nommé RG ("*Residential Gateway*"). L'un des deux porte les informations d'authentification (identificateur et mot de passe). Cette machine terminale ou bien se petit routeur se connecte au réseau et parle à un AN ("*Access Node*" : dans le cas de l'ADSL, c'est le DSLAM qui sert d'AN, dans le cas d'un accès commuté, c'est le serveur de modems). L'authentification pourrait être faite par l'AN. Mais l'utilisateur ne parle pas toujours au même AN (par exemple s'il est mobile) et puis, on gagne en souplesse en découplant les fonctions d'accès et d'authentification. On a donc un serveur qui stocke les informations d'authentification et les paramètres des clients, le AAA ("*Authentication, Authorization and Accounting*"). Entre l'AN et le AAA se trouve souvent un NAS ("*Network Access Server*"), un routeur IP (dans certains cas, AN et NAS sont confondus, par exemple pour la plupart des serveurs PPP). Le NAS est client RADIUS et utilise ce protocole pour demander à l'AAA « j'autorise ce client? » L'AAA, serveur RADIUS, répond oui ou non et ajoute une série d'**attributs**, qui sont les paramètres de la session, par exemple l'adresse IP à utiliser. Notez que RADIUS ne sert qu'entre le NAS et le AAA. Entre le RG et le NAS, on peut utiliser plusieurs autres protocoles, comme PPP ou, plus courant aujourd'hui, DHCP (RFC 3315¹).

RADIUS avait déjà des attributs pour IPv6 : le RFC 3162 avait `Framed-IPv6-Prefix` pour indiquer le préfixe IPv6 à utiliser et `Framed-Interface-Id` qui, combiné avec la valeur précédente, permettait

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc3315.txt>

de fabriquer une adresse IPv6 pour l'utilisateur (cette séparation puis recombinaison était plus adaptée à PPP qu'à DHCP, qui donne des adresses entières). Et le RFC 4818 avait `Delegated-IPv6-Prefix` qui permettait de transmettre un préfixe à déléguer à un routeur par l'option de délégation DHCP du RFC 3633.

Quels sont ces attributs qui manquaient dans les RFC 3162 et RFC 4818? La section 3 en fournit la liste, et ils sont désormais notés dans le registre IANA <<https://www.iana.org/assignments/radius-types>> (cf. section 6). Le premier est `Framed-IPv6-Address` qui permet d'attribuer une adresse IPv6 complète au visiteur (a priori via DHCP). Elle peut apparaître dans les réponses RADIUS, mais aussi dans les questions, pour exprimer un souhait (que le serveur RADIUS peut ignorer). `Framed-IPv6-Address` peut être envoyé dans une réponse RADIUS en même temps que les anciens `Framed-IPv6-Prefix` and `Framed-Interface-Id` (par exemple si le réseau local, derrière le RG, utilise à la fois DHCP et l'auto-configuration sans état - SLAAC).

Le second attribut, `DNS-Server-IPv6-Address`, indique l'adresse IP d'un résolveur DNS. (Un seul résolveur ; mais la réponse RADIUS peut contenir plusieurs attributs `DNS-Server-IPv6-Address`, afin de transmettre les adresses de plusieurs résolveurs.) Ces serveurs DNS peuvent ensuite être indiqués aux machines du réseau local par les "*Router Advertisement*" du RFC 8106 ou bien en DHCP (RFC 3646).

Ensuite, `Route-IPv6-Information` permet de spécifier une route statique. L'attribut existant, `Framed-IPv6-Route` (RFC 3162), ne suffit pas car elle est pour l'usage du NAS, il ne la transmet pas au RG. Au contraire, le nouvel attribut `Route-IPv6-Information` est prévu pour être redistribué. Le NAS pourra transmettre cette information au RG avec les annonces "*Router Advertisement*" du RFC 4191 ou bien une méthode équivalente. Les autres données nécessaires dans l'option "*Route Information*" de l'annonce (par exemple la préférence ou la durée de vie), devront être connues du NAS par un autre moyen (ce point a été le plus chaud lors des discussions dans le groupe de travail).

Enfin, dernier attribut, `Delegated-IPv6-Prefix-Pool` indique le nom d'un "*pool*" d'adresses IPv6 à utiliser par le NAS. Là encore, c'est un attribut RADIUS conçu pour être relayé avec DHCP mais qui peut coexister avec `Framed-IPv6-Pool`, plutôt fait pour les "*Router Advertisement*".