

RFC 4861 : Neighbor Discovery for IP version 6

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 septembre 2007. Dernière mise à jour le 24 novembre 2008

Date de publication du RFC : Septembre 2007

<https://www.bortzmeyer.org/4861.html>

Voici une nouvelle version du protocole ND ("*Neighbor Discovery*") qui permet à une machine IPv6 de trouver l'adresse MAC d'une autre machine qui se trouve sur le même réseau local.

Lorsqu'une machine veut écrire à une autre machine située sur le même lien et qu'elle ne connaît que son adresse IP, son adresse de couche 3, comment fait-elle pour avoir l'adresse MAC, l'adresse de couche 2 qu'il faut mettre, par exemple, dans l'en-tête de la trame Ethernet ?

IPv4 utilisait ARP, spécifié dans le RFC 826¹. Ce protocole avait plusieurs limites, notamment le fait qu'il n'utilisait pas IP, requérant des machines qu'elles mettent donc en œuvre un autre protocole. IPv6 a donc un mécanisme assez différent, ND, qui fonctionne au dessus d'ICMP v6 et donc d'IP.

ND permet aux machines de trouver les routeurs, aux routeurs de s'annoncer, et aux machines de trouver leurs voisines. Voici quelques paquets vus avec `tcpdump -n ip6`. D'abord, un routeur se signale en écrivant à l'adresse "*multicast*" `ff02::1`, « toutes les machines » :

```
15:20:02.032894 fe80::201:96ff:fe96:dc60 > ff02::1: icmp6: router advertisement [class 0xe0]
```

(Cette fonction de ND n'était pas en IPv4 gérée par ARP mais par "*Router Discovery*", RFC 1256.) Maintenant, on a le même routeur qui cherche à joindre `2001:660:3003:3::1:3` et qui diffuse donc une demande de voisin ("*neighbor solicitation*") :

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc826.txt>

```
15:19:37.981830 fe80::201:96ff:fe96:dc60 > ff02::1:ff01:3: icmp6: neighbor solicitation: who has 2001:660:3003:3::1
```

Ici, la machine n'avait jamais répondu. Ici, un cas où la machine sollicitée, 2001:660:3003:3::1:1, répond :

```
15:30:44.416346 fe80::211:43ff:fee7:bcde > 2001:660:3003:3::1: icmp6: neighbor sol: who has 2001:660:3003:3::1
15:30:44.417438 2001:660:3003:3::1 > fe80::211:43ff:fee7:bcde: icmp6: neighbor adv: tgt is 2001:660:3003:3::1
```

On note que le solliciteur écrit toujours depuis son adresse « lien local » ("*link-local*").

Naturellement, les résultats d'une découverte du voisin sont gardés dans un cache, qu'on peut afficher. Sur Linux :

```
% ip neigh show
fe80::210:dbff:feb8:e5ed dev eth0 lladdr 00:10:db:b8:e5:ed router REACHABLE
2001:660:3003:3::1 dev eth0 lladdr 00:10:db:b8:e5:ed router REACHABLE
fe80::219:b9ff:fee4:2987 dev eth0 lladdr 00:19:b9:e4:29:87 router REACHABLE
```

Sur FreeBSD :

```
% ndp -na
Neighbor                               Linklayer Address  Netif  Expire      S  Flags
2001:470:1f15:121:223:12ff:fe56:b34d  0:23:12:56:b3:4d   sis1  20h24m25s  S
...
```

La section 6.2.1 du RFC précise qu'un routeur doit fournir un moyen de configurer les paramètres qui sont utilisés dans la découverte de voisin qu'il effectue et dans les annonces du RFC 4862. Avec le logiciel radvd <<http://www.litech.org/radvd/>>, cela se fait dans `/etc/radvd.conf` qui peut ressembler à (radvd utilise pour ses options exactement les noms suggérés par le RFC) :

```
...
prefix 2001:DB8:49::/64
{
    AdvOnLink on;
    AdvPreferredLifetime 1800;
}
```

Et on voit alors avec un `tcpdump -vvv` le paramètre « durée de vie » ("*ltime*" pour "*life time*") :

```
18:25:59.264392 fe80::204:75ff:fece:efbe > ff02::1: icmp6: router advertisement(chlim=64, pref=medium, route=)
```

Peu de changements par rapport au RFC 2461 et ils portent essentiellement sur la sécurité. L'ancien RFC ne la mentionnait guère, sauf pour expliquer que le protocole était peu sûr (les risques sont détaillés dans les RFC 3756 et RFC 6104). Désormais, la section Sécurité est plus détaillée et cite des solutions possibles comme le protocole SEND, spécifié dans le RFC 3971. Depuis, une autre est apparue, les gardes, dans le RFC 6105.