

*afnic*

# Sécurité d'IPv6

*Stéphane Bortzmeyer*

AFNIC

*bortzmeyer@nic.fr*

*afnic*

# Sécurité d'IPv6

*Stéphane Bortzmeyer*

AFNIC

*bortzmeyer@nic.fr*

*afnic*

2/24

# Introduction

- IPv6 est la version d'IP normalisée en 1995-1998 (RFC 2460)
- Principale motivation, avoir davantage d'adresses IP. Permet de retrouver l'adressage, donc les communications, de bout en bout. Les bricolages IPv4, genre CGN, ne fournissent pas cela.
- Déploiement plutôt lent et laborieux (par exemple, bien des enseignants ne parlent toujours que d'IPv4 en cours)
- Des évolutions depuis dix ans : pas mal d'articles sur des problèmes de sécurité d'IPv6 sont maintenant dépassés.

## Nouveautés techniques d'IPv6 intéressantes pour la sécurité

- Adresses plus longues (128 bits). A des conséquences pour le *scan* ou pour les pare-feux avec état.
- Auto-configuration sans état possible (mais pas obligatoire). Les routeurs émettent des RA (*Router Advertisement*) sur le réseau local. Les machines combinent le préfixe du réseau, appris dans le RA, avec un suffixe (par exemple dérivé de l'adresse MAC).

# Appréciation générale

## IPv6, c'est IP

Cela veut dire que 95 % des questions de sécurité sont les mêmes en IPv4 et IPv6.

Cet exposé est spécifique à IPv6 et se focalise donc sur les 5 % restants. Mais ne perdez pas de vue ce chiffre de 95 % !

## Les 95 % communs

- Usurpation d'adresse IP source triviale (OK, il y a les CGA du RFC 3972, mais c'est très peu utilisé)
- Pas d'authentification ou de chiffrement par défaut, au niveau IP (IPsec est peu déployé)
- Attaques par déni de service volumétriques (force brute)
- Attaques contre les protocoles de transport (*TCP SYN flood*) ou contre les applications (CMS en PHP ou Java...)
- Protocoles de résolution d'adresses sur le réseau local différents (ARP vs. NDP) mais posant des problèmes similaires

# Les 5 % restants

- 1 Entre v4 et v6, il y a des différences **contingentes** qui sont liées à l'état **actuel** des mises en œuvre et aux compétences actuelles des administrateurs. Celles-ci vont disparaître avec le temps.
- 2 Et il y a des différences qui sont des différences de protocole (et resteront donc pour toujours),
- 3 Certaines de ces différences sont en faveur d'IPv4, d'autres d'IPv6 et d'autres encore sont neutres.

## Différences contingentes

- 1 Configuration incohérente, exemple une ACL en v4 sans équivalent en v6 (en 2013, des gens font encore les ACL à la main ???),
- 2 Logiciels limités (exemple : un pare-feu qui gère IPv4 mais pas IPv6),
- 3 Logiciels peu performants (exemple : un pare-feu qui gérerait IPv4 dans les ASIC mais IPv6 en logiciel),
- 4 Logiciels bogués (marchent bien en IPv4 mais n'ont jamais été réellement testés au feu en IPv6),
- 5 Techniques de transition/coexistence compliquées et qui viennent avec de nouveaux risques,
- 6 Administrateurs incompetents (par exemple parce qu'ils croient à tort qu'IPv6 est différent d'IPv4).
- 7 Heureusement, les attaquants aussi sont incompetents. On ne voit quasiment jamais d'attaques en IPv6, même lorsqu'il y a des vulnérabilités énormes.

# Exemple du retard du déploiement d'IPv6

J'ai reçu mon premier spam en IPv6 en 2012 seulement. Mes serveurs SSH font l'objet d'innombrables tentatives de connexion en IPv4 et **jamais** en IPv6 (alors que fail2ban n'est pas installé en v6...).

Donc, IPv6 a de vrais atouts en sécurité :-)

## État des logiciels

Pour quasiment tous les logiciels, c'est moins bon ou équivalent en IPv6

- Pare-feux. Ne gèrent pas IPv6 ou le font lentement (*slow path*). Pas toujours adaptés au grand nombre d'adresses (table pour le filtrage à état).
- Bogues. Exemple : envoyer un RA avec **beaucoup** de préfixes listés tue Mac OS X, dont les programmeurs ne connaissaient pas la notion de dépassement de tableau  
`http://samsclass.info/ipv6/proj/RA_flood2.htm`

# Un contre-exemple : Netfilter

Le pare-feu de Linux marche très bien en IPv6 (mais je ne jurerais pas qu'il ait 100 % des fonctions qu'il a en v4).

```
ip6tables -A INPUT --protocol tcp --dport ssh --jump ACCEPT
ip6tables -A INPUT --jump REJECT
```

Tout ce qui n'est pas SSH sera bloqué. Sur le client :

```
From 2a01:e35:8bd9:8bb0:ba27:ebff:feba:9094 \
    icmp_seq=8 Destination unreachable: Port unreachable
```

*afnic*

11 / 24

## Netfilter avec des fonctions plus avancées

On va limiter le trafic ICMP echo (ping) :

```
ip6tables -A INPUT -p icmpv6 --icmpv6-type echo-request \
    -m hashlimit --hashlimit-name ICMP \
    --hashlimit-above 1/second --hashlimit-burst 1 \
    --hashlimit-mode srcip \
    --hashlimit-srcmask 64 -j DROP
```

On teste en envoyant 10 p/s :

```
ping6 -i 0.1 2001:db8:8bd9:8bb0:ba27:ebff:feba:9094
```

Et on constate effectivement une limitation à 1 p/s :

```
81 packets transmitted, 8 received, 90% packet loss, time 8577ms
```

Essayez-cela sur un pare-feu commercial et revenez me dire si ça a marché.

*afnic*

12 / 24

# Sécurité des techniques de transition

Techniques souvent à base de tunnels, avec aucune sécurité et des possibilités d'usurpation supplémentaires

**Teredo est particulièrement vulnérable. Ne l'utilisez pas.**

6to4 est à peine meilleur. Lire le RFC 6180

Ces vulnérabilités sont souvent celles de tous les tunnels (donc exploitables en v4 pur)

# Différences de protocole

**Certains différences ne vont pas disparaître avec le temps**

Elles relèvent de vraies différences entre IPv4 et IPv6. Là encore, certaines sont favorables à IPv6, d'autres à IPv4.

# RAcailles

- 1 Les RA (annonces des routeurs), comme DHCP, ne sont pas sécurisées/authentifiées.
- 2 Comme avec DHCP, une machine peut jouer au routeur et émettre des RAcailles (*rogue RA*). Problème décrit dans le RFC 6104.
- 3 Comme avec DHCP, la meilleure protection semble être du filtrage par le commutateur (*RA Guard*, RFC 6105) : services appelés *IPv6 First Hop Security* chez Cisco, par exemple

# Vie privée et adresse MAC

- 1 Par défaut, le mode le plus courant de configuration d'une adresse est automatique, avec le préfixe au début et un dérivé de l'adresse MAC à la fin.
- 2 Si on change de réseau, on garde l'adresse MAC et on peut donc être suivi. À noter que les gens qui se plaignent de ce risque sont probablement les mêmes qui utilisent Facebook et acceptent tous les cookies.
- 3 Solution : adresses aléatoires (RFC 4941).
- 4 Mise en œuvre dans tous les systèmes (pas forcément activée par défaut).

# Analyse des en-têtes

- 1 Des tas de logiciels de sécurité ont besoin de « sauter » l'en-tête du paquet, pour aller au contenu. En IPv4, c'est pénible (en-tête de taille variable) mais connu.
- 2 En IPv6, nombre quelconque d'en-têtes et, jusqu'à récemment, pas de gabarit commun → impossible à analyser <http://www.bortzmeyer.org/analyse-pcap-ipv6.html>. Ajouter un seul en-tête suffit parfois pour échapper à la détection.
- 3 Depuis le RFC 6564, un algorithme fiable est possible.
- 4 Les commentaires dans le code source de Wireshark ou Net : :Pcap ne sont pas flatteurs pour IPv6. . .
- 5 Attention aussi à la fragmentation (RFCs en cours pour insister sur le risque).

# Énumération des adresses

- 1 En IPv4, balayer **toutes** les adresses est réaliste (un /16 en moins de 2 h, à 10 adr./s). Cela permet de trouver des machines discrètes.
- 2 En IPv6, une telle énumération **naïve** est hors de question (un /64 prendrait des milliards d'années).
- 3 Cela ne veut pas dire qu'on ne peut pas être trouvé : adresses prévisibles ( . . . : : 1), connexions sortantes. . . Le RFC 5157 donne plein d'idées.

## Plus de NAT ? Moins de sécurité ?

- En IPv4, le NAT est quasi-indispensable (manque d'adresses).
- En IPv6, le NAT n'est pas indispensable (mais permis, RFC 5902 et 6296).
- Le NAT sera-t-il déployé en IPv6 ? On ne le sait pas encore.
- Est-ce que cela aura des conséquences sur la sécurité ?
- Le NAT n'apporte **pas** de sécurité <http://www.bortzmeyer.org/nat-et-securite.html>.
- En IPv6 comme en IPv4, les outils de sécurité sont du code correct, des pare-feux, des utilisateurs prudents.

## Et c'est tout ?

Non, il y a encore des tas de points à voir mais on manque de temps.

J'ai cité les plus importants. Pour approfondir, IPV6\_V6ONLY dans les applications

<http://stackoverflow.com/a/2798432/15625>,

l'attaque *Neighbor cache* [http://inconcepts.biz/~jsw/IPv6\\_NDP\\_Exhaustion.pdf](http://inconcepts.biz/~jsw/IPv6_NDP_Exhaustion.pdf),

le filtrage d'ICMP « pour des raisons de sécurité » qui est une énorme erreur en IPv6 et bien d'autres ...

# Mesures à prendre

Plutôt que de se demander gravement « IPv6 est-il plus ou moins sûr ? »...

Mieux vaut parler de mesures concrètes de sécurité.

« Ne pas déployer IPv6 » n'est pas une bonne idée : on a besoin de ces adresses en plus. En prime, IPv6 tourne peut-être déjà sur votre réseau local.

## Mesures

- Connaître son réseau : déployer des outils équivalents à l'arpwatch d'IPv4 comme ndpmon  
<http://ndpmon.sourceforge.net/> ou ramond ou rafxid.
- Vérifier que les outils de sécurité comme l'IDS, gèrent aussi IPv6. **Ne pas hésiter à demander aux fournisseurs sinon !**
- Le système SEND sécurise les RA par certificats cryptographiques et signatures. Très complexe et très peu déployé.

# Conclusion : IPv6 est-il plus ou moins sûr ?

- 1 Peu de différences
- 2 Mais, en sécurité, il faut connaître ces différences

## Références

- 1 Il existe relativement peu de références solides sur la sécurité d'IPv6 (mais pas mal de trucs produits par des trolls).
- 2 RFC 6092 et 6204 : recommandation de filtrage dans les *boxes* de M. Michu. Attention, documents nuancés.
- 3 Pas mal de RFC en cours de travail ou de publication sur des problèmes concrets (comme le fait que les RA avaient le droit d'être fragmentés).