RFC 1918 : Address Allocation for Private Internets

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 novembre 2007

Date de publication du RFC : Février 1996

http://www.bortzmeyer.org/1918.html

Depuis longtemps, le manque d'adresses IPv4 se fait sentir. Pour obtenir ces précieuses adresses, il faut remplir de longs documents à envoyer au RIR, ou bien payer son FAI pour une offre « pro » ou n'importe quel autre qualificatif indiquant que, entre autres, on aura d'avantage d'adresses, peut-être un /29 au lieu d'un simple /32 (pour les politiques d'allocation, voir le RFC 7020[1]). D'où la demande pour un stock d'adresses IPv4 **privées**, non annoncées sur l'Internet et non uniques globalement, mais dans lequel on pourrait piocher à loisir. C'est ce que propose ce RFC, certainement un des plus cités, le "1918" étant devenu synonyme de ressource privée.

Ce RFC est court et pourrait se contenter de lister (section 3) les trois préfixes privés réservés :
— 10.0.0.0/8
— 172.16.0.0/12
— 192.168.0.0/16, certainement le plus utilisé des trois.
Et les bases des RIR, accessibles via whois, reflètent bien cette réservation à l'IANA :

```
% whois  10.42.0.1

OrgName:    Internet Assigned Numbers Authority
OrgID:      IANA
Address:    4676 Admiralty Way, Suite 330
City:       Marina del Rey
StateProv:  CA
PostalCode: 90292-6695
Country:    US

NetRange:   10.0.0.0 - 10.255.255.255
CIDR:       10.0.0.0/8
NetName:    RESERVED-10
NetHandle:  NET-10-0-0-0-1
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7020.txt

```
Parent:
NetType:    IANA Special Use
NameServer: BLACKHOLE-1.IANA.ORG
NameServer: BLACKHOLE-2.IANA.ORG
Comment:    This block is reserved for special purposes.
Comment:    Please see RFC 1918 for additional information.
Comment:
RegDate:
Updated:    2002-09-12
...
```

Mais l'idée même d'adresses IP privées ne s'est pas imposée sans mal. Un des principes d'architecture de l'Internet est en effet la **connectivité de bout en bout**. Toute machine peut parler directement à toute autre. C'est l'une des grandes innovations de l'Internet, tous les réseaux concurrents à l'époque (années 1970 et 80) n'envisageaient que des réseaux isolés. Or, s'il existe des adresses privées, elles ne sont pas **globalement uniques**. Deux machines sur des sites différents peuvent avoir la même adresses `192.168.1.1`. Cela remet donc en cause le modèle de base et le prédécesseur de notre RFC, le RFC 1597 avait été fortement critiqué, notamment dans le RFC 1627, intitulé "*Network 10 Considered Harmful*".

Notre RFC détaille donc aussi, dans ses sections 2 et 4, les motivations de ces adresses privées et explique pourquoi on ne peut pas s'en passer.

Si la poussière soulevée par le débat est bien retombée par la suite, c'est parce qu'on envisageait un déploiement rapide d'IPv6 qui règlerait le problème, grâce à son abondance d'adresses. Ce déploiement ne s'étant pas (encore ?) produit, notre RFC et ses adresses privées continuent à bénéficier d'un grand succès.

Ce succès s'étend même à des domaines non prévus, comme la documentation, qui devrait normalement utiliser `192.0.2.0/24` (cf. RFC 5737).

Pourquoi ces trois préfixes-là et pas d'autres ? Pour `10.0.0.0/8` la raison semble connue mais pas pour les autres <http://serverfault.com/questions/64013/>.

Parfois, ces adresses privées « sortent » même, par accident, du réseau local où elles auraient dû rester confinées, malgré la section 5 du RFC qui explique qu'il ne faut pas le faire. On doit donc prendre soin de les filtrer. Les règles d'ACL d'un coupe-feu commencent souvent par quelque chose du genre (ici, des règles de Netfilter dans le noyau Linux) :

```
Chain norfc1918 (2 references)
target     prot opt source               destination
rfc1918    all  --  172.16.0.0/12        0.0.0.0/0
rfc1918    all  --  192.168.0.0/16       0.0.0.0/0
rfc1918    all  --  10.0.0.0/8           0.0.0.0/0
...
Chain rfc1918 (6 references)
target     prot opt source               destination
LOG        all  --  0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 6 prefix `Shorewall:rfc1918:D
DROP       all  --  0.0.0.0/0            0.0.0.0/0
```

(Dans le cas ci-dessus, les règles sont ajoutées automatiquement par Shorewall <http://www.bortzmeyer.org/filtrage-avec-shorewall.html>.)

De même, un routeur BGP refuse en général de ses pairs des annonces pour ces préfixes (ici, la syntaxe d'IOS) :

```
! http://www.cymru.com/Bogons/index.html
! Deny any packets from the RFC 1918 netblocks to block
! attacks from commonly spoofed IP addresses.
access-list 2010 remark Anti-bogon ACL
! Bogons
access-list 2010 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 2010 deny ip 192.168.0.0 0.0.255.255 any log-input
```

Et le nombre de serveurs DNS faisant des requêtes de type PTR pour ces adresses, et fatiguant ainsi pour rien les serveurs de `in-addr.arpa`, a nécessité le déploiement d'un système dédié pour les absorber, l'AS112.

Aujourd'hui, le petit réseau local typique a donc presque toujours des adresses tirées du RFC 1918, un routeur NAT et/ou des relais applicatifs et une seule adresse IP publique, attribuée par le FAI.