Un cas compliqué d'utilisation d'un préfixe AfriNIC en dehors de l'Afrique

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 février 2013. Dernière mise à jour le 19 février 2013

https://www.bortzmeyer.org/usage-prefixe-afrinic.html

On le sait, les adresses IPv4 sont désormais épuisées <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html> dans la plupart des régions du monde et pas mal de sites n'ont toujours pas déployé IPv6, rendant cette pénurie pénible. Il est donc tentant, plutôt que de faire l'effort d'un passage à IPv6, d'aller chercher des adresses IPv4 là où il y en a encore, notamment en Afrique. On a souvent dit que des entreprises extérieures au continent allaient « faire leurs courses » en Afrique en créant une filiale bidon qui allait demander à AfriNIC des adresses qui seraient ensuite annoncées ailleurs. Mais, là, c'est plus amusant, c'est un préfixe qui fait partie de la réserve AfriNIC mais qui n'est pas enregistré via AfriNIC.

Commençons par le commencement : un service français nommé Qwant fait pas mal de publicité (avec même l'aide d'une ancienne ministre) et annonce un site Web en http://www.qwant.com/. L'adresse IP correspondante peut être trouvée facilement <https://dns.bortzmeyer.org/www.qwant.com/A> et vaut 154.45.216.7. Toute adresse IP utilisée sur l'Internet fait partie d'un réseau qui est documenté publiquement, via le protocole whois. Est-ce le cas ici ?

```
% whois 154.45.216.7
% This is the AfriNIC Whois server.

% Note: this output has been filtered.

% Information related to '154.0.0.0 - 154.255.255.255'

inetnum:        154.0.0.0 - 154.255.255.255
netname:        AFRINIC-20090508
...
```

On est renvoyé à AfriNIC mais, là, il n'y a rien, aucune déclaration correspondant à ce réseau. Il n'est pas affecté. C'est tout à fait anormal. Creusons un peu.

Le préfixe `154.0.0.0/8` vu ci-dessus est bien à AfriNIC. On le voit à l'IANA en regardant la liste des allocations <https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml> où on lit {154/8; Administered by AFRINIC; (depuis) 1993-05; whois.afrinic.net}. Notez la date : le préfixe a été utilisé avant car, en 1993, AfriNIC n'existait pas (Wayback Machine montre qu'en 2003, ce préfixe était encore "*various registries*" <http://web.archive.org/web/20030603174522/https://www.iana.org/assignments/ipv4-address-space>). Mais, aujourd'hui, il est censé être entièrement chez AfriNIC, avec toutefois des affectations qui avaient été faites avant. Le RIR africain n'a pas affecté de blocs dans ce préfixe, comme on le voit en regardant la liste des affectations aujourd'hui <ftp://ftp.afrinic.net/pub/stats/afrinic/delegated-afrinic-20130218>. On y voit que la délégation sous `154.0.0.0/8` n'a pas encore commencé, ce qui est normal, AfriNIC ayant encore plusieurs /8 <http://www.afrinic.net/fr/statistiques/epuisement-dipv4>. Mais c'est bien cette réserve importante (alors qu'APNIC et le RIPE-NCC ont épuisé la leur) qui peut en tenter certains.

Bon, mais alors comment se fait-il que ce préfixe fantôme fonctionne ? C'est parce qu'il n'y a nul besoin qu'un préfixe soit enregistré pour fonctionner. N'importe qui peut annoncer n'importe quoi, surtout si personne d'autre ne le fait. On peut voir l'annonce du préfixe englobant `154.45.216.7` par plusieurs moyens :

```
% bgproute 154.45.216.7
AS path: 3130 2914 174
Route: 154.40.0.0/13
```

Ou par des services sur le Web comme chez Hurricane Electric <http://bgp.he.net/net/154.40.0.0/13> ou au RIPE-NCC <http://www.ris.ripe.net/mt/prefixdashboard.html?prefix=154.40.0.0%2F13>. Conclusion en regardant ce qui se passe dans le monde des routes annoncées en BGP : enregistré ou pas, documenté via whois ou pas, `154.40.0.0/13` est bien vivant, il est annoncé par Cogent (l'AS 174), depuis au moins 2006 (je ne sais pas si les statistiques remontent pas au delà) et il fonctionne (on peut joindre cette adresse). traceroute nous montre que le site est bien chez Cogent, dans les environs de Paris :

```
% traceroute 154.45.216.7
traceroute to 154.45.216.7 (154.45.216.7), 30 hops max, 60 byte packets
 1  freebox (192.168.2.254)  10.117 ms  10.100 ms  10.091 ms
 2  88.189.152.254 (88.189.152.254)  36.830 ms  36.834 ms  36.835 ms
 3  78.254.1.62 (78.254.1.62)  38.480 ms  38.490 ms  38.491 ms
 4  rke75-1-v900.intf.nra.proxad.net (78.254.255.42)  38.395 ms  38.399 ms  41.759 ms
 5  cev75-1-v902.intf.nra.proxad.net (78.254.255.46)  40.177 ms  41.744 ms  41.764 ms
 6  * * *
 7  th2-crs16-1-be1002.intf.routers.proxad.net (212.27.57.217)  35.829 ms  64.348 ms  66.053 ms
 8  th2-9k-1-be1000.intf.routers.proxad.net (212.27.59.206)  30.479 ms  30.481 ms  30.473 ms
 9  * ix-15-547.tcore1.PVU-Paris.as6453.net (195.219.241.173)  32.592 ms  32.603 ms
10  te0-0-0-23.ccr21.par04.atlas.cogentco.com (130.117.15.33)  36.124 ms te0-7-0-23.ccr21.par04.atlas.cogent
11  te0-5-0-2.mpd22.par01.atlas.cogentco.com (154.54.58.233)  41.341 ms te0-6-0-4.mpd22.par01.atlas.cogentco
12  te1-1.ccr01.par05.atlas.cogentco.com (130.117.1.70)  42.823 ms te8-1.ccr01.par05.atlas.cogentco.com (154
13  te2-1.ccr01.par13.atlas.cogentco.com (154.54.61.90)  101.346 ms  99.259 ms  99.253 ms
14  * * *
15  * * *
...
```

S'agit-il d'un « vol », d'un « détournement » ? Ce n'est pas si simple. D'abord, personne d'autre n'est titulaire de ce préfixe. Son utilisation par Cogent et son client Qwant ne gêne donc personne, tant qu'AfriNIC ne commence pas à utiliser ce préfixe (auquel cas il faudra faire attention à ces allocations du

passé). Ensuite, certes, il n'y a aucune trace de l'enregistrement de ces adresses dans les bases AfriNIC mais AfriNIC est quand même au courant puisque le domaine DNS `45.154.in-addr.arpa` (servant aux résolutions d'adresses en noms) est bien délégué par AfriNIC à Cogent. Peut-être y a-t-il simplement eu un cafouillage, facilité par l'héritage ancien de ce préfixe. On constate en effet que le serveur whois d'ARIN, lui, renvoie chez Cogent (notez la date) :

```
% whois -h whois.arin.net 154.45.216.7
...
NetRange:       154.45.0.0 - 154.45.255.255
CIDR:           154.45.0.0/16
OriginAS:       AS174
NetName:        COGENT-154-45-16
NetHandle:      NET-154-45-0-0-1
Parent:         NET-154-0-0-0-0
NetType:        Direct Assignment
RegDate:        1992-02-05
...

Found a referral to rwhois.cogentco.com:4321.

%rwhois V-1.5:0010b0:00 rwhois.cogentco.com
154.45.216.7
network:ID:NET4-9A2DD8001C
network:Network-Name:NET4-9A2DD8001C
network:IP-Network:154.45.216.0/28
network:Postal-Code:75008
network:Country:FR
network:City:Paris
network:Street-Address:11 Rue Marbeuf
network:Org-Name:Qwant
network:Tech-Contact:ZC108-ARIN
network:Updated:2012-03-01 18:16:32
network:Updated-by:Bill Garrison
```

Quelles conclusions en tirer ? D'abord, que d'être absent (ou mal présent) des bases des RIR, et donc de la plupart des IRR, n'empêche pas un préfixe de fonctionner (le serveur du RIPE lui voit une visibilité quasi-parfaite). Ensuite que le marais (les adresses affectées avant le système des RIR) est mal rangé <`https://www.bortzmeyer.org/nettoyage-marais.html`>. Enfin, que l'Internet est quand même très complexe.

Le problème avait été trouvé à l'origine par arapaho <`https://twitter.com/Grosquik/status/303498753288060928`>. Merci à Jean-Philippe Pick pour son aide pour l'analyse. Merci aussi à Stephen D. Strowes pour son voyage dans le temps, et aux équipes de Cogent et d'AfriNIC pour des réponses rapides et correctes.