Le RIPE-NCC va-t-il nettoyer le marais des adresses IP ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 novembre 2011

https://www.bortzmeyer.org/nettoyage-marais.html

À la réunion RIPE de Vienne, le 1er novembre, Axel Pawlik, directeur du RIPE-NCC a fait un exposé sur « "*What to do about IPv4 Legacy Address Space*" » ou que faire du **marais**, ces préfixes IP alloués il y a de nombreuses années, bien avant que les RIR n'existent. Il y a de nombreux préfixes dont le statut juridique et opérationnel est... peu clair.

Aujourd'hui, normalement, les choses sont précises : les RIR comme le RIPE-NCC allouent des adresses IP à leurs membres, les LIR ("*Local Internet Registry*"), qui sont typiquement des opérateurs ou des FAI. Cette allocation se fait suivant tout un tas de règles soigneusement mises par écrit et qui détaillent le statut juridique des adresses allouées. Le tout est ensuite publié par le RIR (on y accède typiquement via whois), pour que chacun puisse savoir qui gère quelle partie de l'Internet, et comment le contacter.

Ça, c'est aujourd'hui. Mais autrefois, avant que les RIR existent, à l'époque où journalistes, avocats et ministres ne connaissaient pas l'Internet ? Eh bien, les adresses IP étaient allouées aussi, mais on gardait moins de paperasse, c'était souvent informel, et les organisations qui s'en occupaient ont parfois disparu et parfois changé de métier. Par exemple, en Europe, il y avait souvent des NIR ("*National Internet Registry*") qui servaient d'intermédiaire entre RIR et LIR, et qui ont tous abandonné cette activité. Les adresses qu'ils géraient sont donc parfois dans un limbe juridico-politique. Quant aux titulaires de ces adresses IP du lointain passé, il ont souvent oublié eux-même qu'ils en avaient, ou alors ils ne s'occupent pas des enregistrements qui moisissent dans les bases des RIR, sans être jamais mis à jour. Ce sont ces préfixes alloués dans les temps pré-RIR qu'on appelle **le marais** ("*the swamp*") ou, plus gentiment, **l'héritage** ("*the legacy*").

Voyons quelques exemples (tous sont publics et n'importe qui peut les voir en utilisant un client whois sur le serveur du RIPE-NCC, `whois.ripe.net`, ou encore via l'interface Web dudit NCC, en <https://apps.db.ripe.net/search/query.html>). D'abord, le préfixe `192.134.12.0/24`. whois nous dit :

```
inetnum:      192.134.12.0 - 192.134.12.255
...
country:      FR
admin-c:      KA774-RIPE
tech-c:       KA774-RIPE
status:       EARLY-REGISTRATION
mnt-by:       ERX-NET-192-134-12-MNT
```

Le statut "*EARLY REGISTRATION*" (alias ERX) est un des signes de l'appartenance de ce préfixe au marais. Alloué dans un quasi-vide juridique, `192.134.12.0/24` flotte... Le mainteneur de l'objet (l'entité autorisée à apporter des modifications) a été créé et mis automatiquement par le RIPE-NCC (les anciens objets de la base RIPE n'avaient pas ce concept de mainteneur). Est-il à jour, ainsi que les contacts ? whois nous dit :

```
address:      FR
...
e-mail:       ASHK@frined51.bitnet
```

Une adresse de courrier électronique Bitnet, ça, c'est un "*collector*"... Ce réseau ne fonctionne plus depuis de longues années. Cela indique clairement que l'objet n'est pas géré. Il n'est pas non plus utilisé (aucune route n'y mène).

Autre exemple, `192.93.12.0/24`, qui illustre un autre problème. Lors de la création des RIR, il n'a pas été évident d'affecter chaque objet de la base à un RIR et certains l'ont été deux fois <`https://www.bortzmeyer.org/conflit-numeros-as.html`>. Ce préfixe contient donc des informations issues des deux bases. Non protégé, il a été automatiquement verrouillé par le RIPE-NCC <`http://www.ripe.net/internet-coordination/news/announcements/deprecation-of-the-none-authenticati`> comme l'indique la présence du mainteneur `RIPE-NCC-LOCKED-MNT`. Le récupérer ne sera donc pas une mince affaire. Si on regarde le contact, on constate des numéros de téléphone à huit chiffres, ce qui indique bien l'absence d'entretien. Comme le précédent, ce préfixe ne semble pas utilisé, il n'apparaît pas dans les tables de routage publiques.

Enfin, dernier exemple, `192.93.232.0/24` est alloué à une société qui semble avoir purement et simplement disparu. (Il existe une société de même nom mais qui semble n'avoir aucun rapport. Pour en être sûr, il faudrait une vraie enquête sur place, ce qui dépasse les moyens et l'envie des RIR.)

Tous ces exemples concernent la France mais le marais est bien sûr présent dans tous les pays de l'OCDE (ceux qui ont été les premiers à se précipiter sur l'Internet et à obtenir des adresses IP).

Alors, après cette longue introduction, qu'a annoncé Axel Pawlik à Vienne ? Le lancement d'une campagne pour, dans un premier temps, améliorer l'enregistrement des informations sur ces préfixes du marais. L'idée est d'encourager les titulaires de ces adresses à enfin mettre à jour les informations contenues dans la base du RIR. Le RIPE-NCC, après des années d'inaction sur ce sujet, a fait les choses en grand, sorti une jolie brochure « "*Legacy space in the RIPE-NCC service region*" », annoncé la création d'une équipe dédiée, joignable par courrier à `legacy@ripe.net`, et appelé sur son site Web <`http://www.ripe.net/lir-services/resource-management/legacy-space`> à nettoyer le marais.

Pourquoi cette soudaine activité ? Parce que l'épuisement des adresses IPv4 <`https://www.bortzmeyer.org/epuisement-adresses-ipv4.html`> transforme le marais en or : ces adresses non gérées et souvent non utilisées deviennent tout à coup très valables. Comme l'a dit clairement Pawlik, mêlant la carotte (« "*Show you are a good Internet citizen*" ») et le bâton, ces adressses manifestement abandonnées

sont des cibles tentantes pour des détourneurs... Pawlik n'a pas explicitement dit que ces adresses pourraient être récupérées par le RIPE-NCC un jour mais on peut penser que c'est une étape ultérieure possible.

Cela ne veut pas dire que tout soit rose si on « régularise » sa situation. Le RIPE-NCC, émanation des opérateurs réseaux, peut aussi en profiter pour « suggérer » qu'on confie désormais ses adresses à un LIR, transformant ainsi des adresses qui étaient, de fait, indépendantes du fournisseur en adresses qui « appartiendront » désormais à un opérateur.

Les conseils que je donnerai donc aux gens qui sont titulaires de préfixes IP du marais :

— D'abord et avant tout, faites un inventaire exact de vos ressources virtuelles comme les adresses IP. Beaucoup d'organisations découvrent par hasard (par exemple à l'occasion de l'arrivée d'un nouvel ingénieur) qu'elles sont les heureuses titulaires d'un /24.
— Ensuite, examinez bien les enregistrements dans la base RIPE. Sont-ils à jour ?
— Enfin, déterminez leur statut et, en fonction de celui-ci, décidez d'une stratégie pour les mettre à jour, limitant ainsi le risque qu'un détourneur ne vous les arrache. Prévoyez du temps, de l'aspirine et des tranquillisants. Lorsque toutes les informations dans la base (noms des personnes, adresses, numéros de téléphone) sont obsolètes, prouver que vous êtes bien le titulaire va être un parcours du combattant.

Ne laissez pas un objet dans la base du RIPE avec des informations dépassées, même si la mise à jour va être longue et pénible ! Un tel objet est une invitation au détournement.

À noter que l'alerte avait déjà été donnée par exemple sur la liste IP <https://listes.services.cnrs.fr/wws/arc/ip/2010-12/msg00003.html>. Si vous voulez fouiller vous-même dans la base du RIPE-NCC, un outil pratique est leur recherche plein texte <https://apps.db.ripe.net/search/full-text.html>. La base est également téléchargeable en FTP sur ftp.ripe.net:/ripe/dbase.

La question se pose aussi dans les autres régions et, en Amérique du Nord, la NSF (qui gérait le réseau académique états-unien qui formait une bonne partie de l'Internet à cette époque) affirme <http://www.internetgovernance.org/2012/09/22/its-official-legacy-ipv4-address-block-hold
que les adresses IP allouées à cette époque appartiennent bien à leurs titulaires et que le RIR nord-américain, ARIN, créé bien après, n'a aucun droit de les réclamer.