

Faudra t-il désormais noter l'adresse IP et le port ?

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 Novembre 2009

<http://www.bortzmeyer.org/loguer-adresse-et-port.html>

Les serveurs réseau qui tournent aujourd'hui enregistrent leur activité dans un journal où ils notent, en général, l'adresse IP de leur client. Vue l'évolution de l'Internet va t-il falloir également enregistrer le port dudit client ?

N'importe quel serveur réseau aujourd'hui, qu'il fasse du HTTP, du SMTP ou bien d'autres protocoles reposant sur TCP, note chaque connexion dans son journal. Par exemple, pour Apache, les entrées dans le journal ressemblent à :

```
192.0.2.235 - - [12/Nov/2009:15:38:31 +0100] "GET /feed.atom HTTP/1.0" 304 - "-" "Liferea/1.4.23 (Linux; fr_FR.U
2001:db8:2f58:ce40:216:3eff:feb0:452f - - [12/Nov/2009:15:38:36 +0100] "GET /xml-to-csv.html HTTP/1.1" 200 18011
```

où 192.0.2.235 et 2001:db8:2f58:ce40:216:3eff:feb0:452f sont les adresses IP de deux clients. On enregistre l'adresse IP car elle permet, normalement, d'identifier de manière unique une machine. C'est en tout cas l'architecture originale de l'Internet.

Cette idée qu'une adresse IP est unique est largement répandue, y compris chez les non-techniciens. Par exemple, Cédric Manara (<http://www.cedricmanara.com/>) attire mon attention sur un arrêt d'un tribunal, le 7 octobre 2009 à Paris (http://www.legalis.net/jurisprudence-decision.php3?id_article=2758), qui dit « les numéros IP étant attribués par l'IANA (Internet Assigned Numbers Agency [sic]), deux ordinateurs ne peuvent pas avoir la même adresse IP ».

L'affirmation n'est pas 100 % fausse mais elle est très simpliste et ne correspond plus à la réalité de l'Internet d'aujourd'hui.

D'abord, il faudrait préciser « deux ordinateurs ne peuvent pas avoir la même adresse IP **en même temps** » car les adresses IP sont couramment réaffectées. C'est probablement ce que fait Verizon (gérant de l'adresse citée dans le jugement).

Ensuite, l'IANA n'a pas de force de police et ne peut donc pas empêcher des gens de prendre sauvagement des adresses IP. À une époque, un opérateur européen s'était ainsi arrogé un préfixe IP qui fut finalement officiellement alloué à un opérateur kenyan. Avec l'épuisement des adresses IPv4 (<http://www.bortzmeyer.org/epuisement-adresses-ipv4.html>), ce genre de squattage sera de plus en plus fréquent.

Un problème analogue est que l'architecture de l'Internet ne permet pas de s'assurer facilement de l'authenticité d'une adresse IP, vieux problème de sécurité bien connu (voir le RFC 2827¹). Avec UDP, utiliser une fausse adresse est trivial. C'est toutefois plus compliqué en TCP, qui est utilisé pour le courrier, ce qui affaiblit l'argument de la défense qui laissait entendre que n'importe qui pouvait facilement usurper une adresse.

Tout ceci est bien connu. Mais il y a un autre problème, plus récent. Le principe d'un espace d'adresse unique, commun à tout l'Internet, ne correspond plus à la réalité d'aujourd'hui. Avec les adresses IP privées du RFC 1918, (ce qui n'est pas le cas de celle citée, attention), des milliers d'ordinateurs ont la même adresse et utilisent ensuite le NAT. En Europe ou aux États-Unis, le partage ne concerne en général qu'un foyer ou qu'une entreprise (et donc tous les ordinateurs partageant cette adresse sont sous la même responsabilité). Mais, avec l'épuisement rapide des adresses IPv4, cela va changer et des NAT au niveau d'un opérateur entier, déjà courants en Asie ou en Afrique, vont se répandre.

Ce partage intensif d'adresses IP est tellement répandu que l'IETF, à sa réunion d'Hiroshima (<http://www.ietf.org/meeting/76/>), s'est penchée sérieusement sur une normalisation du fait que l'identificateur, aujourd'hui, n'est plus l'adresse seule mais le couple adresse+port (<http://www.ietf.org/proceedings/09nov/agenda/aplusp.html>) (merci à Rémi Desprès pour la discussion sur ce sujet). Un des documents qui discutent la question est l'"Internet-Draft" `draft-ford-shared-addressing-issue`. Mais il y en a d'autres comme `draft-ietf-geopriv-held-identity-extensions` qui note « *"However, widespread use of network address translation (NAT) means that some Devices cannot be uniquely identified by IP address alone."* ».

Revenons à notre journal. Tout cela veut dire que cela sera de moins en moins utile d'enregistrer uniquement l'adresse IP. Il faudra bientôt enregistrer également le port source utilisé par le client, et, si on veut de la traçabilité, que le routeur NAT conserve trace des correspondances entre une adresse IP interne et le couple {adresse IP publique, port} qu'il avait attribué à cette adresse interne. Verra t-on Apache écrire :

```
192.0.2.235:13174 - - [12/Nov/2009:15:38:31 +0100] "GET /feed.atom HTTP/1.0" 304 - "-" "Liferea/1.4.23 (Linux; U; Linux; en; rv:1.9.1.3; Firefox/3.5.3; ID:db8:2ff58:ce40:216:3eff:feb0:452f):48221 - - [12/Nov/2009:15:38:36 +0100] "GET /xml-to-csv.html HTTP/1.0" 200 1024
```

où 13174 et 48221 sont les ports source ? Apache ne savait pas autrefois (http://onlamp.com/pub/a/apache/2004/04/22/blackbox_logs.html?page=3) enregistrer le port mais c'est possible désormais (merci à Tony Finch) en mettant dans le format `%{remote}p` (%p étant le port local au serveur). Les applications Web, elles, peuvent utiliser la variable CGI `REMOTE_PORT`.

(Notez la syntaxe légèrement différente pour IPv6, décrite dans la section 3.2 du RFC 3986. Ceci dit, le partage d'adresses n'ayant pas de raison d'être avec IPv6, vue l'abondance d'adresses, le problème ne devrait pas exister.)

¹Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc2827.txt>