

Grande perturbation de l'Internet ce sept novembre...

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 novembre 2011

<https://www.bortzmeyer.org/crash-internet-nov-2011.html>

Ce lundi 7 novembre 2011, vers 14h05 UTC, grande perturbation de la Force. Des tas de destinations deviennent injoignables sur l'Internet...

Voici par exemple un des graphes montrant une brusque diminution du trafic (les heures sont des heures locales, pas UTC) : . À noter qu'un second plantage, moins important, a eu lieu vers 15h30 UTC. On voit bien l'effet des deux plantages sur ce graphique de DNSmon <<http://dnsmon.ripe.net/>>, qui montre l'impact de la panne sur les serveurs DNS de .fr (le serveur c.nic.fr a été le plus impacté) :

Les utilisateurs ne peuvent plus travailler <<http://www.mondespersistants.com/news/eve-online-deconne20234/>> et plein de gens se plaignent.

Le problème venait d'une annonce BGP amusante qui a planté (et fait redémarrer) certains routeurs Juniper. Voir les annonces Twitter d'Absolight <<https://twitter.com/#!/Absolight/status/133555827859664896>> et de Neo <<https://twitter.com/#!/NeoTelecoms/status/133560203898654720>>. Cela ressemble donc beaucoup à des problèmes comme celui de l'attribut 99 <<https://www.bortzmeyer.org/bgp-attribut-99.html>>. Même si c'était plutôt Cisco qui nous avait habitué à ce genre de crashes de grand style.

La bogue ne touchait apparemment que la gamme MX, en version 10.2, 10.3 et certaines 10.4 de JunOS; Raphaël Maunier me dit que les plus basses versions **non** affectées sont les 10.4R6, 11.1R4 et 11.2R1). La bogue est apparemment enregistré chez Juniper sous l'identificateur PSN-2011-08-327 <<http://pastebin.com/HBWih92j>> (j'ai mis un lien vers un "pastebin" car le rapport officiel est réservé aux clients de Juniper <<https://twitter.com/#!/JuniperNetworks/status/133637820081389568>>; à tout hasard, je garde une copie de PSN-2011-08-327 ici (en ligne sur <https://www.bortzmeyer.org/files/juniper-PSN-2011-08-327.txt>)).

Une bonne façon de voir d'un coup d'œil qu'il y a eu une grande perturbation BGP est de regarder les archives de RouteViews du mois en cours <<http://archive.routeviews.org/bgpdata/2011>.

11/UPDATES/> (merci à Jared Mauch pour la bonne idée). Pour novembre 2011, regardez les fichiers `updates.20111107.1415.bz2` et `updates.20111107.1430.bz2` (le nom du fichier donne l'heure en UTC), vingt fois plus gros que la normale et montrant une avalanche de mises à jour BGP suite au crash de tant de routeurs.

C'est l'occasion de se rappeler que la résilience de l'Internet est un combat permanent <<https://www.bortzmeyer.org/eteindre-internet.html>>. Ainsi, l'un des opérateurs affectés, Level 3 a une part du marché telle que ses pannes entraînent la coupure d'une bonne partie de l'Internet.

Quelques ressources utiles pour les administrateurs réseaux confrontés à ce genre de problèmes :

- La liste "*Outages*" <<https://puck.nether.net/mailman/listinfo/outages>> et sa liste des observatoires <<http://wiki.outages.org/index.php/Dashboard>> (ce qui suppose qu'assez de liens Internet fonctionne pour qu'on l'atteigne...).
- L'"*Internet Health Report*" <<http://www.internetpulse.net/>>.
- Le "*Internet Traffic Report*" <<http://www.internettrafficreport.com/>>, dont j'ai extrait l'image ci-dessus qui montre la baisse de trafic.

Autres articles sur cette panne :

- Interview de Raphaël Maunier <<http://www.zdnet.fr/actualites/raphael-maunier-neotelecom.htm>>, de NeoTelecoms
- Contrairement à ce que prétend l'article de ZDnet <<http://www.zdnet.fr/actualites/grosse-perturbation-d-internet-causee-par-une-panne-des-routeurs-juniper-3976543.htm>>, cela n'a rien à voir avec une mise à jour du logiciel des routeurs (cela serait amusant que tout le monde ait fait la mise à jour en même temps, mais le journaliste incompetent a confondu « "*BGP update*" » - mise à jour des tables de routage - avec « "*software update*" » - mise à jour du logiciel).