La panne Facebook du 4 octobre 2021

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 octobre 2021. Dernière mise à jour le 5 octobre 2021

https://www.bortzmeyer.org/facebook-octobre-2021.html

Aujourd'hui, Facebook a connu une panne importante. Que s'est-il passé ? On sait désormais que la cause racine était un problème de configuration des routeurs BGP. A-t-on des détails ?

Le message d'erreur de beaucoup d'utilisateurs :

Je vous le dis tout de suite, je n'ai pas d'informations internes à Facebook, et je n'ai pas fait une longue enquête. N'attendez donc pas de révélations extraordinaires. Commençons par les faits. Aujourd'hui, lundi 4 octobre vers 1550 UTC, les services de Facebook, y compris WhatsApp et Instagram étaient en panne. (La panne a duré environ 6 heures.) Les utilisateurs avaient typiquement un message faisant allusion au nom de domaine, qui ne marchait pas.

Arrivé là, il faut se rappeler que les noms de domaine et le protocole DNS sont critiques pour le fonctionnement de l'Internet. Quasiment toute activité sur l'Internet commence par une requête DNS. Si elle ne fonctionne pas, presque rien n'est possible. Mais il faut aussi se rappeler que ce DNS ne fonctionne pas sur un réseau parallèle : il utilise l'Internet lui aussi, les paquets DNS circulent dans des paquets IP et que donc un problème affectant IP va souvent se manifester comme un problème DNS (puisque c'est par le DNS qu'on commence une session).

Demandons aux sondes RIPE Atlas <https://atlas.ripe.net/> de trouver les serveurs de noms de facebook.com :

```
% blaeu-resolve -r 200 --type NS facebook.com
[a.ns.facebook.com. b.ns.facebook.com. c.ns.facebook.com. d.ns.facebook.com.] : 97 occurrences
[ERROR: SERVFAIL] : 48 occurrences
[] : 3 occurrences
Test #32421708 done at 2021-10-04T16:16:14Z
```

Une partie y arrive, probablement parce que l'information était encore dans la mémoire de leur résolveur <https://www.bortzmeyer.org/resolveur-dns.html>. Mais ce n'est pas le cas de toutes. En effet, pendant la panne, les serveurs DNS faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> pour facebook.com ne répondaient pas. Voici la liste de ces serveurs, obtenue avec dig en demandant à un serveur de la zone parente, .com (on ne pouvait pas faire un dig « normal » puisque le résolveur <https://www.bortzmeyer.org/resolveur-dns.html> qu'il utilise aurait essayé de joindre les serveurs en panne) :

```
% dig @a.gtld-servers.net. A a.ns.facebook.com.

; <<>> DiG 9.16.15-Debian <<>> @a.gtld-servers.net. A a.ns.facebook.com.
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4686
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 9
...
;; AUTHORITY SECTION:
facebook.com. 172800 IN NS a.ns.facebook.com.
facebook.com. 172800 IN NS b.ns.facebook.com.
facebook.com. 172800 IN NS c.ns.facebook.com.
facebook.com. 172800 IN NS d.ns.facebook.com.
...
;; ADDITIONAL SECTION:
a.ns.facebook.com. 172800 IN A 129.134.30.12
a.ns.facebook.com. 172800 IN AAAA 2a03:2880:f0fc:c:face:b00c:0:35
...
;; Query time: 16 msec
;; SERVER: 2001:503:a83e::2:30#53(2001:503:a83e::2:30)
;; WHEN: Mon Oct 04 18:24:55 CEST 2021
;; MSG SIZE  rcvd: 833
```

Maintenant, demandons aux sondes RIPE Atlas d'interroger un de ces serveurs, a.ns.facebook.com :

```
%  blaeu-resolve -r 200 --type NS --nameserver 129.134.30.12 --nsid facebook.com
Nameserver 129.134.30.12
[] : 3 occurrences
[TIMEOUT] : 189 occurrences
Test #32421749 done at 2021-10-04T16:25:09Z
```

On le voit, l'échec est total. Un peu plus tard, ça marche un peu mieux :

```
%  blaeu-resolve -r 200 --type NS --nameserver 129.134.30.12 --nsid facebook.com
Nameserver 129.134.30.12
[TIMEOUT] : 192 occurrences
[ERROR: SERVFAIL] : 3 occurrences
[a.ns.facebook.com. b.ns.facebook.com. c.ns.facebook.com. d.ns.facebook.com.] : 1 occurrences
Test #32421800 done at 2021-10-04T16:35:54Z
```

Donc, les choses sont claires : les serveurs DNS faisant autorité ne marchaient pas. Cela explique la panne vue par les utilisateurs. Maintenant, pourquoi ces quatre serveurs (et davantage de machines physiques, en raison de l'"*anycast*") seraient-ils tous tombés en même temps ? Il y a plusieurs hypothèses, comme une erreur de configuration propagée automatiquement à toutes les machines (automatiser les

configurations simplifie la vie mais les erreurs ont des conséquences plus graves). Mais on peut noter autre chose : tous ces serveurs sont dans le même AS, le 32934, l'AS de Facebook. Un problème de routage dans l'AS, empêchant les paquets d'arriver, peut également empêcher les serveurs DNS de répondre. Mettre tous ses œufs dans le même panier est décidément une mauvaise pratique. (Notez que ZoneMaster <https://zonemaster.fr/> teste cette mauvaise pratique et vous alerte <https://twitter.com/benoit_ampeau/status/1445108785329147907>.) C'est un problème connu, déjà signalé par le RFC 2182 [1], en 1997…

Creusons cette idée. Plusieurs observateurs ont noté que les préfixes IP de Facebook ont subitement disparu de la DFZ. Cela explique que les serveurs DNS soient devenus injoignables. Les sondes RIPE Atlas montrent que les traceroute ne vont pas très loin, les préfixes n'étant plus annoncés :

```
% blaeu-traceroute -r 10 --format 129.134.30.12
Measurement #32421753 Traceroute 129.134.30.12 uses 10 probes
9 probes reported
Test #32421753 done at 2021-10-04T16:26:49Z
From:  89.152.207.6    2860    NOS_COMUNICACOES, PT
Source address:  89.152.207.6
Probe ID:  1001047
1    ['!', '!', '!']
2    10.137.196.193    NA    NA    [10.743, 10.446, 6.726]
3    10.255.48.82    NA    NA    [12.727, 15.974, 14.397]
4    ['*', '*', '*']
5    ['*', '*', '*']
6    ['*', '*', '*']
7    ['*', '*', '*']
8    ['*', '*', '*']
255    ['*', '*', '*']

From:  188.254.182.226    43205    BULSATCOM-BG-AS Sofia, BG
Source address:  192.168.88.13
Probe ID:  15646
1    192.168.88.1    NA    NA    [0.66, 0.415, 0.4]
2    188.254.180.1    43205    BULSATCOM-BG-AS Sofia, BG    [1.552, 1.614, 1.231]
3    46.40.64.1    43205    BULSATCOM-BG-AS Sofia, BG    [2.223, '*', '*']
4    ['*', '*', '*']
5    ['*', '*', '*']
6    ['*', '*', '*']
7    ['*', '*', '*']
8    ['*', '!', '!', '!', '!', '!', '!', '*', '*']
255    ['*', '*', '*']
```

Des préfixes IP plus généraux sont parfois restés. Ainsi, le `129.134.30.0/24` d'un des serveurs a disparu mais un /17 plus générique est resté. On voit ici (source : RIPEstat <https://stat.ripe.net/widget/bgp-update-activity#w.starttime=2021-09-21T11%3A00%3A00&w.endtime=2021-10-05T11%3A00%3A00&w.resource=129.134.30.0%2F24>, le retrait du /24 puis son rétablissement (`129.134.30.0/23`, `129.134.31.0/24` et bien d'autres avaient subi le même sort) :

La panne DNS semble donc avoir été une conséquence d'une fausse manœuvre BGP. Cela explique, par exemple, que le service Tor de Facebook, `facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.o` ne marche pas non plus (il ne dépend pas du DNS, `.onion` est spécial).

Le réseau social Instagram pendant la panne. Bien que ses serveurs DNS répondaient parfaitement, le serveur Web dépend de Facebook :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2182.txt`

Plusieurs personnes sur les réseaux sociaux ont également noté que tous les serveurs faisant autorité pour `facebook.com` étaient sous le même domaine (`ns.facebook.com`). Ce n'est pas forcément une mauvaise idée. Certes, cela oblige à publier des colles (les adresses IP des serveurs), ce qui complique l'administration. Et, si le domaine en question a un problème, par exemple administratif, cela frappe tous les serveurs. D'un autre côté, cela évite de dépendre de tiers, ce qui est pourquoi cette pratique est parfois recommandée (par exemple par l'ANSSI <https://www.ssi.gouv.fr/guide/bonnes-pratiques-pour-lacquisition-et-lexploitation-de-noms-de-domaine/>).

En revanche, il était tout à fait justifié de noter que les TTL de Facebook sont anormalement bas : 300 secondes. Cela veut dire que si la panne dure plus de 5 minutes, ce qui a été le cas, les mémoires des résolveurs ne servent plus à rien. La robustesse du DNS nécessite des TTL bien plus longs (supérieurs à la durée d'une panne typique).

Ah, et puis rappelez-vous que Facebook n'est pas tout l'Internet : tous les autres services fonctionnaient parfaitement (sauf ceux qui avaient choisi de dépendre de Facebook).

Articles dans les médias :

— Numérama <https://www.numerama.com/tech/744753-instagram-messenger-facebook-et-wh
html>
— Très bonnes explications, très pédagogiques, de Cécile Morange <https://twitter.com/AtaxyaNetwork/
status/1445096685286350849>, sous forme d'un fil Twitter.
— Bon article de synthèse sur Numérama <https://www.numerama.com/tech/744948-pourquoi-faceb
html>.
— Le communiqué officiel de Facebook (en anglais) <https://engineering.fb.com/2021/10/04/networking-traffic/outage/> ; la panne a été causée par un problème de configuration de leurs routeurs BGP. Facebook a ensuite considérablement détaillé dans un excellent article <https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/>.
— Comme d'habitude, excellent article de Cloudflare (en anglais) <https://blog.cloudflare.com/october-2021-facebook-outage/>, avec plein de détails techniques concrets et des explications pédagogiques.
— Un autre article très détaillé, par Qrator (en anglais) <https://radar.qrator.net/blog/giants_fall_aftershock>, notamment sur les observations BGP.
— ZDnet (en anglais) <https://www.zdnet.com/article/what-took-facebook-down-major-global>

La panne vue par l'excellent service de vérification DNSviz <https://dnsviz.net/> (le même résultat, en ligne <https://dnsviz.net/d/facebook.com/YVsrkg/dnssec/>) :