Coupure de l'Internet en Égypte

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 janvier 2011. Dernière mise à jour le 2 février 2011

http://www.bortzmeyer.org/egypte-coupure.html

Quelques jours après que je publie un article posant la question « Peut-on éteindre l'Internet <http://www.bortzmeyer.org/eteindre-internet.html> », le dictateur Moubarak a décidé d'illustrer un des points de l'article : oui, on peut couper l'Internet localement, pendant un temps relativement long (au moins plusieurs jours). L'Égypte a donc été presque totalement privée d'Internet du 28 janvier au 2 février.

Comme d'habitude lors de ce genre d'événements, on ne sait pas grand'chose, ce qui n'empêche pas les informations erronées. Ainsi, un article de la BBC <http://www.bbc.co.uk/news/technology-12306041> explique que la coupure s'est faite sur la base du DNS, ce qu'aucun fait observé ne permet de dire. Bien au contraire, le phénomène, vu de l'extérieur, montre que la censure a frappé plus bas, du côté des couches 1 à 3. En effet, même de l'extérieur, alors qu'on n'a pas besoin du DNS, on ne va pas très loin. Ici, depuis le réseau de Verizon aux États-Unis, en visant un des serveurs DNS de `.eg` :

```
% traceroute FRCU.EUN.eg
traceroute to FRCU.EUN.eg (193.227.1.1), 30 hops max, 60 byte packets
 1  192.sub-66-174-112.myvzw.com (66.174.112.192)  66.711 ms  67.259 ms  67.439 ms
 2  66.174.112.255 (66.174.112.255)  76.192 ms  76.588 ms  76.931 ms
 3  81.sub-66-174-13.myvzw.com (66.174.13.81)  77.121 ms  85.802 ms  86.028 ms
 4  98.sub-66-174-12.myvzw.com (66.174.12.98)  89.049 ms  86.694 ms  113.811 ms
 5  90.sub-66-174-9.myvzw.com (66.174.9.90)  116.961 ms  116.436 ms  113.944 ms
 6  87.sub-66-174-9.myvzw.com (66.174.9.87)  123.913 ms  73.061 ms  70.609 ms
 7  253.sub-69-83-16.myvzw.com (69.83.16.253)  84.492 ms  84.283 ms  93.580 ms
 8  xe-7-1-0.edge3.Washington1.Level3.net (4.59.144.25)  94.144 ms !N  93.805 ms !N  94.264 ms !N
```

Le !N signifiant "*Network Unreachable*" et, comme on n'a pas quitté les États-Unis, on voit que les routeurs de Level 3, privés d'informations BGP, ne savent plus où envoyer les paquets. Un coup d'œil sur le service RIS du RIPE-NCC <http://www.ris.ripe.net/mt/prefixinuse-result.html?prefix=193.227.1.1&preftype=LSPEC&rrc_id=1000&interval=1&outype=html&submit=Search&.submit=type> le confirme : le préfixe n'est plus du tout visible (cela va et ça vient : il est parfois à nouveau annoncé, puis supprimé).

Pour une présentation générale du problème en français, l'article de 20 minutes <http://www.20minutes.fr/article/660896/web-couper-internet-pays-comme-egypte-prend-2-minutes> est satisfaisant. Un peu plus technique, celui de Rue89 <http://www.rue89.com/2011/01/28/pour-faire-taire-les-opposants-legypte-coupe-internet-187888>. Quelles sont les bonnes sources pour les détails techniques ? Les habituelles, le blog de Renesys <http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml>, ExtraExploit <http://extraexploit.blogspot.com/2011/01/egypt-telecom-as-isolation-bgplay-show.html>, les RIPE labs <http://labs.ripe.net/Members/akvadrako/live_eqyptian_internet_incident_analysis> et BGPmon <http://bgpmon.net/blog/?p=450>. Ces articles ne sont pas forcément d'accord entre eux. Par exemple, le nombre de préfixes IP égyptiens varie de 2900 à 3500 mais cet écart est normal : il n'y a pas de moyen simple et fiable de décider si tel préfixe est en Égypte ou ailleurs, le routage dans l'Internet n'étant pas basé sur la nationalité. Un certain nombre des « préfixes égyptiens qui fonctionnent toujours » sont donc probablement situés dans d'autres pays. À noter également qu'il n'y a que 129 préfixes égyptiens alloués par AfriNIC mais un préfixe n'est pas forcément égal à une route, en raison, entre autres, de la désagrégation, de l'utilisation de préfixes alloués par un autre RIR, etc.

Autres intéressants articles sur la coupure égyptienne, les statistiques BGP du RIPE <http://stat.ripe.net/egypt/>, et des graphes par le même RIPE-NCC <http://labs.ripe.net/Members/rbarnes/visualizing-the-egyptian-disconnection>.

Comme l'a noté Renesys, le réseau de l'opérateur NOOR semble encore largement accessible. Contrairement à ce que j'avais pu écrire au début, il semblerait que les liaisons physiques sont toujours là. On peut voir les préfixes qu'il annonce sur un "*looking glass*" comme <http://www.robtex.com/as/as20928.html#bgp> ou bien <https://www.dan.me.uk/bgplookup?asn=20928&include_downstream=on>. Cela permet de trouver assez facilement une adresse IP égyptienne qui répond toujours par exemple la 217.139.5.1, qui répond à ping et à traceroute :

```
traceroute to 217.139.5.1 (217.139.5.1), 30 hops max, 60 byte packets
 1  192.sub-66-174-112.myvzw.com (66.174.112.192)  173.370 ms  173.406 ms  173.519 ms
 2  66.174.112.255 (66.174.112.255)  173.607 ms  175.010 ms  176.161 ms
 3  81.sub-66-174-13.myvzw.com (66.174.13.81)  315.883 ms  316.606 ms  316.478 ms
 4  98.sub-66-174-12.myvzw.com (66.174.12.98)  317.190 ms  316.777 ms  318.488 ms
 5  * 90.sub-66-174-9.myvzw.com (66.174.9.90)  320.371 ms *
 6  87.sub-66-174-9.myvzw.com (66.174.9.87)  319.318 ms  327.311 ms  337.118 ms
 7  253.sub-69-83-16.myvzw.com (69.83.16.253)  452.587 ms  301.666 ms  307.929 ms
 8  xe-7-1-0.edge3.Washington1.Level3.net (4.59.144.25)  308.167 ms  280.718 ms  280.341 ms
 9  vlan80.csw3.Washington1.Level3.net (4.69.149.190)  221.054 ms  221.299 ms  105.477 ms
10  ae-82-82.ebr2.Washington1.Level3.net (4.69.134.153)  105.679 ms  217.237 ms  216.963 ms
11  ae-4-4.ebr2.Newark1.Level3.net (4.69.132.102)  218.182 ms  217.496 ms  218.182 ms
12  ae-23-52.car3.Newark1.Level3.net (4.68.99.39)  218.974 ms  218.595 ms  218.196 ms
13  TELECOM-ITA.car3.Newark1.Level3.net (4.71.148.10)  219.340 ms  218.955 ms  235.213 ms
14  ge15-0.palermo6.pal.seabone.net (195.22.218.211)  475.708 ms  472.234 ms  472.138 ms
15  noor.palermo6.pal.seabone.net (195.22.198.34)  432.727 ms  431.700 ms  431.638 ms
16  * * *
17  217.139.5.1 (217.139.5.1)  431.051 ms  431.587 ms  431.142 ms
```

(Seabone est un service de Telecom Italia, qui gête entre autres un câble méditerranéen et on voit qu'on a pu aller jusqu'à Palerme, puis en Égypte.)

J'avais parlé du domaine de tête .eg. Fonctionne t-il toujours ? Oui, car un seul de ses serveurs est situé en Égypte. Les deux autres, aux États-Unis et en Autriche, continuent à répondre, bonne illustration de la résilience du DNS :

```
% check_soa eg
There was no response from FRCU.EUN.eg
RIP.PSG.COM has serial number 2010100421
NS5.UNIVIE.AC.AT has serial number 2010100421
```

Évidemment, sans route pour acheminer les paquets ensuite, cela n'a que peu d'intérêt...

Quelle leçon à en tirer sur la résilience de l'Internet ? (Voir aussi l'interview de Benjamin Bayart sur PublicSénat <http://www.publicsenat.fr/lcp/politique/egypte-coupure-d-internet-prend-quelques
D'abord, que l'Égypte a peu d'opérateurs internationaux et peu de liens physiques vers l'extérieur. Cela facilite la censure (juste quelques coups de téléphone à donner) et cela augmente également la vulnérabilité de l'Internet égyptien aux coupures accidentelles comme l'avait montré la grande panne de 2008 <http://www.renesys.com/blog/2008/01/mediterranean_cable_break.shtml>. Aujourd'hui, la situation n'a pas trop changé (voir une jolie carte <https://secure.wikimedia.org/wikipedia/en/wiki/File:Cable_map18.svg>) et on peut se demander qu'elle est la part de la pauvreté (qui empêche de multiplier les liens), de la géopolitique (qui rend peu envisageable des passages par la Libye ou par Israël), de l'incompétence ou du calcul cynique (moins de liens égal un réseau plus contrôlable).

Et à l'intérieur de l'Égypte, que se passe t-il ? On n'a pas beaucoup de témoignage pour l'instant. La question de savoir si l'Internet d'un pays peut fonctionner en autonomie, déconnecté de l'Internet mondial, a déjà fait l'objet de plusieurs discussions. Ici, pour ne prendre que le cas du DNS, l'Égypte a deux serveurs DNS racine au Caire (les serveurs F et J, à noter que, au moins pour F, son administrateur n'y a plus accès depuis l'extérieur), ainsi qu'un serveur de .com donc il est possible qu'un Internet égyptien isolé puisse continuer à fonctionner.

J'ai reçu un témoignage d'un français installé en Égypte et qui connaît un peu les réseaux : il semble bien que la coupure touchait aussi l'intérieur. Je le cite « Le gouvernement a coupé plusieurs choses, en plusieurs jours. Dans l'ordre : les SMS sur les mobiles ne sont plus passés, puis les communications voix, puis la 3G. Le gouvernement espérait que cela diminuerait les manifs mais devant la foule dans les manifs, le téléphone mobile a été rétabli. Actuellement, on peut m'appeler sans trop de problème, mais je ne peux plus appeler vers l'étranger. Apparemment les communications intérieures fonctionnent. Ensuite seulement, ils ont coupé l'accès Internet. Au bureau, on a l'ADSL. Le réseau "physique" était toujours actif (je voyais la diode ADSL normalement) mais sur l'ordinateur, je n'accédais à rien : pas de sites étrangers et même pas de sites locaux. Tout était coupé. »

Et la reprise ? Elle s'est faite le 2 février, vers 1100 UTC. On trouve des observations sur cette reprise en :

- L'analyse de BGPmon <http://bgpmon.net/blog/?p=480>,
- Les statistiques du RIPE <http://stat.ripe.net/egypt/>,
- Celle de Renesys <http://www.renesys.com/blog/2011/02/egypt-returns-to-the-internet.shtml>. Cet article, et le précedent, pointent le retard du réseau académique égyptien à revenir, alors qu'il héberge le serveur de noms primaire de .EG.

Une des raisons pour lesquelles la dictature égyptienne a rétabli la connexion à l'Internet est peut-être de pure finance : selon un article du Monde, citant l'OCDE <http://www.lemonde.fr/technologies/article/2011/02/03/egypte-la-coupure-internet-a-coute-90-millions-de-dollars_1474489_651865.html>, cette coupure aurait coûté très cher à l'économie égyptienne.