Concevoir un réseau informatique mondial

Stéphane Bortzmeyer

Capitole du Libre

14 Novembre 2026

Le succès peut cacher les alternatives

- L'Internet est aujourd'hui partout,
- Il a écrasé ses concurrents,
- On ne parle plus d'OSI ou de X.25 qu'avec commisération,
- Mais le succès éclipse le fait que d'autres choix auraient été possibles.
- « Nous vous rappelons qu'il existe d'autres possibilités. »

Faire un réseau en partant de zéro ?

- Régulièrement, des gens viennent expliquer que l'Internet est nul et qu'ils ont des idées géniales,
- Premier obstacle : la base installée et son inertie,
- Mais si on fait table rase ? Si on repart de zéro ?
- Cela a peu de chances d'être adopté mais c'est intellectuellement intéressant.

L’ingéniérie, ce sont toujours des compromis

- Il n’y a pas de solution idéale,
- Il faut choisir entre des solutions imparfaites,
- C’est très net en sécurité : les gens qui râlent contre le 2FA seront toujours les premiers à protester en cas de piratage.

Le rôle du cahier des charges

- Tout dépend de ce qu'on veut,
- Exemple : la messagerie. Le courrier de l'Internet permet d'écrire à quelqu'un sans introduction préalable,
- C'est très puissant mais ça permet le spam,
- Si on impose une introduction, que perd t-on en spontanéité ?
- Les tenants d'un « meilleur Internet », fait en partant de zéro, dissimulent souvent leur cahier des charges,
- Le cahier des charges est parfois implicite.

Au travail sur le nouveau réseau

- Plein de choix à faire, et pas de repas gratuit,
- Se méfier des yakafokon,
- Concevoir un nouveau réseau : ce que cela implique.

Étude de cas : adresses de taille fixe ou variable ?

- Les adresses IP ont une taille fixe (128 bits),
- Un routeur de cœur doit traiter des millions de paquets à la seconde (donc en matériel, pas en logiciel),
- Inconvénient : si on a mal calculé la taille, la migration va être pénible (IPv4 ➡️ IPv6).

Étude de cas : connecté ou pas connecté ?

- IP utilise des datagrammes : chaque paquet est complètement indépendant,
- Donne le maximum de souplesse au routage,
- Pas d'état dans les routeurs, meilleurs performances et résistance aux pannes,
- Arpanet utilisait des connexions, l'adresse dans les paquets était un court identificateur attribué au début,
- Attention, connexion n'implique pas qu'on fait de la commutation de circuit.

Étude de cas : la sécurité du courrier

- On sait qu'elle est faible (spam, hameçonnage),
- Les techniques de sécurité cassent certains usages (DMARC et les listes de diffusion, les listes de blocage…),
- Et authentifier ne suffit pas,
- Si le courrier avait été sécurisé dès le début, qui l'aurait adopté ? (L'expérience de X.400…)
- Devoir valider les correspondants (cf. Matrix) ?

Étude de cas : la résolution de noms

- L'Internet dépend du DNS,
- Propriétés importantes avec le DNS : unicité des noms, rapidité, dépendance vis-à-vis des parents,
- Cahier des charges : laisser tomber l'unicité ? (Cf. GNUnet ou UUCP.)
- Pair à pair ? OK, mais l'unicité ? Et pas moyen de supprimer `nazi.com`…
- Chaine de blocs ? Techniquement correct (cf. Namecoin) mais plus moyen de changer de politique.

Étude de cas : le routage

- L'Internet dépend de BGP,
- Propriétés importantes : décentralisation presque totale, on peut appliquer sa politique locale, on n'a pas de sécurité par défaut, on ne contrôle pas tout le trajet,
- Difficulté : les relations business entre opérateurs sont très variées,
- Sécurité : la RPKI re-centralise un peu (on n'a rien sans rien).
- Alternatives : Scion ?

Il y a aussi les choix organisationnels

- Pas de chef, pas de Directeur de l'Internet,
- Pas de police, pas de régulateur mondial,
- Décentralisation,
- Difficile de déployer quelque chose (IPv6, DNSSEC, ASPA, une version récente de PHP…).
- Difficile de sécuriser (pas de source unique d'identité, par exemple).

Tor partout, surveillance et censure nulle part ?

- Le serveur connait l'adresse IP du client (et réciproquement), risque de censure et pour la vie privée,
- On aurait pu faire un routage en oignon systématique,
- Performance ?

Micro-paiements

- Bon, c'est dans les couches plus hautes, cette fois,
- Mais l'absence de micro-paiements simples, pas cher, anonymes, a des conséquences pour les créateurs (dépendance vis-à-vis de la pub) et donc pour le contenu.

Si vous voulez faire mieux

- Cahier des charges explicite, et pas uniquement les avantages (comme chantent les *Pretenders* « *something is lost, but something is found* »),
- Bien creuser les conséquences, par exemple en sécurité et en passage à l'échelle,
- Avoir du code qui tourne est un plus : tant qu'on n'a que des *slides* (ou un *tweet*), tout est super.
- Les prétentions marketing du genre « notre système est sécurisé, efficace, convivial, économique, écologique… » seront vues avec méfiance.