RFC 8799 : Limited Domains and Internet Protocols

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 juillet 2020

Date de publication du RFC : Juillet 2020

https://www.bortzmeyer.org/8799.html

Il y a depuis longtemps un débat sur l'architecture de l'Internet : dans quelle mesure faut-il un Internet uniforme, où tout est pareil partout, et dans quelle mesure faut-il au contraire des particularités qui ne s'appliquent que dans telle ou telle partie de l'Internet ? Bien sûr, la réponse n'est pas simple, et ce nouveau RFC explore la question et discute ses conséquences, par exemple pour le développement des normes.

Sur le long terme, la tendance est plutôt au développement de règles locales, et de services qui ne sont accessibles que d'une partie de l'Internet. Le NAS avec les photos de famille accessible uniquement depuis la maison, le site Web permettant aux employés d'indiquer leurs demandes de congés, qu'on ne peut voir que depuis le réseau de l'entreprise, parce qu'on y est présent physiquement, ou bien via le VPN, les lois d'un pays qu'il essaie, avec plus ou moins de succès, d'appliquer sur son territoire...Mais, d'abord, une précision : le terme « local » ne signifie pas forcément une région géographique précise. « Local » peut, par exemple, désigner le réseau d'une organisation spécifique, qui y applique ses règles. « Local » peut être un bâtiment, un véhicule, un pays ou bien un réseau s'étendant au monde entier.

À noter que certains ont poussé cette tendance très loin en estimant que l'Internet allait se fragmenter en réseaux distincts, ne communiquant plus, voire que cela avait déjà été fait. C'est clairement faux, aujourd'hui, comme l'explique bien, par exemple, le RFC 7754 [1], ou bien Milton Mueller dans son livre « *"Will The Internet Fragment ?"* ». On peut toujours visiter ce blog depuis tous les réseaux connectés à l'Internet...

Un petit point de terminologie : le RFC utilise le terme « domaine » pour désigner une région de l'Internet ayant des règles spécifiques. Ce terme ne doit pas être confondu avec celui de « nom de domaine » qui désigne quelque chose de tout à fait différent. « Domaine », dans ce RFC, est plutôt

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7754.txt

utilisé dans le même sens que dans les RFC 6398 et RFC 8085, pour indiquer un « domaine administratif ». C'est un environnement contrôlé, géré par une entité (entreprise, association, individu) et qui peut définir des règles locales et les appliquer.

Aujourd'hui, le concept de « domaine local » ou « domaine limité » n'est pas vraiment formalisé dans l'Internet. Des RFC comme le RFC 2775 ou le RFC 4924 ont plutôt défendu l'inverse, la nécessité de maintenir un Internet unifié, insistant sur le problème des "*middleboxes*" intrusives (RFC 3234, RFC 7663 et RFC 8517). Actuellement, il y a déjà une fragmentation de l'Internet en ilots séparés, puisque certaines fonctions ne marchent pas toujours, et qu'on ne peut donc pas compter dessus. C'est le cas par exemple des en-têtes d'extension IPv6 (RFC 7872), de la découverte de la MTU du chemin (RFC 4821) ou de la fragmentation (RFC 8900). Sans compter le filtrage par les pare-feux. Bref, tous ces problèmes font que, "*de facto*", l'Internet n'est plus transparent, et que des communications peuvent échouer, non pas en raison d'une panne ou d'une bogue, mais en raison de règles décidées par tel ou tel acteur sur le trajet. Donc, en pratique, on a des « domaines limités » mais sans que cela soit explicite, et cela joue un rôle important dans l'utilisation du réseau.

Si on avait des « domaines limités » ou « domaines locaux » explicites, quel serait le cahier des charges de ce concept ? La section 3 du RFC donne quelques idées à ce sujet. Par exemple, ces scénarios sont envisagés :

— Un cas d'usage évident est le réseau de la maison, où des politiques spécifiques à ce logement sont tout à fait légitimes (par exemple, utilisation de Pi-hole pour bloquer les publicités). Typiquement non géré par des professionnels (voire pas géré du tout…), il doit marcher « à la sortie de la boîte ». Le RFC 7368 donne davantage de détails sur cette notion de réseau à la maison.
— Le réseau interne d'une petite entreprise est souvent proche du réseau de la maison : politique locale (donc « domaine limité ») mais personne de compétent pour s'en occuper. Par contre, il est parfois installé par des professionels (mais attention, « professionnel » [Caractère Unicode non montré [2]] « compétent »).
— Sujet à la mode, le réseau dans un véhicule. À l'intérieur du véhicule, il y a des exigences spécifiques, liées à la sécurité, et qui justifient des règles locales.
— Les réseaux SCADA ont également d'excellentes raisons d'avoir une politique locale, notamment en sécurité (cf. RFC 8578).
— Toujours dans le domaine industriel, il y a aussi les réseaux de capteurs et, plus généralement, l'IoT. Ils demandent également des règles locales spécifiques et, en prime, posent parfois des problèmes techniques ardus. C'est encore pire si les objets sont contraints en ressources matérielles (RFC 7228).
— Plus science-fiction, un autre scénario où on ne peut pas suivre les règles de l'Internet public et où il faut des règles locales, les DTN (RFC 4838).
— Les grands réseaux internes d'une organisation, répartie sur plusieurs sites physiques, peuvent également être concernées par le concept de politique locale. Notez qu'un seul RFC parle d'eux, à propos d'IPv6, le RFC 7381.
— Il y a aussi le cas du réseau semi-fermé d'un opérateur. Le réseau est utilisé par des clients de cet opérateur, et celui-ci a une offre réservée à certains, qui propose des garanties de service (avec des techniques comme EVPN ou VPLS). (Le RFC n'en parle pas, mais attention, ici, on commence à s'approcher de la question de la neutralité de l'Internet <https://www.bortzmeyer.org/neutralite.html>.)
— Et enfin (mais je n'ai pas recopié toute la liste du RFC), il y a les centres de données où, là encore, une organisation souhaite avoir une politique locale.

Bref, le cas est fréquent. On se dit, en regardant tous ces scénarios où un réseau, quoique connecté à l'Internet, a de très bonnes raisons d'avoir des règles locales spécifiques, qu'il serait bon qu'une organisation de normalisation, comme l'IETF, trouve une solution générale. Le problème est que, justement, chaque politique locale est différente. Néanmoins, les auteurs du RFC suggèrent de réfléchir à une nouvelle

2. Car trop difficile à faire afficher par LaTeX

façon d'analyser les propositions à l'IETF, en ne considérant pas simplement leur usage sur l'Internet public (le vrai Internet, dirais-je) mais aussi ce qui se passera sur ces domaines limités.

Le RFC cite aussi le cas de protocoles qu'on avait cru pouvoir déployer sur l'Internet public mais qui en fait n'ont marché que dans des environnements fermés. Ce fut le cas bien sûr de RSVP (RFC 2205). Ses auteurs avaient pensé qu'un protocole de réservation de ressources pourrait marcher sur un réseau public, oubliant que, dans ce cas, chaque égoïste allait évidemment se réserver le plus de ressources possibles. (Ce n'est pas un problème spécifique à RSVP : aucun mécanisme de qualité de service ne peut marcher sur un réseau public décentralisé. Imaginez un bit « trafic très important, à ne jamais jeter » ; tout le monde le mettrait à 1 !)

Bon, maintenant qu'on a décrit les scénarios d'usage, quelle(s) solution(s) ? La section 4 du RFC liste quelques exemples de techniques conçues spécialement pour des domaines limités. Notons que le RFC parle des techniques en couche 3, la couche 2 étant évidemment toujours pour un domaine local (encore que, avec TRILL - RFC 6325, la couche 2 peut aller loin). Par exemple :

- DiffServ (RFC 2464), puisque la signification des bits utilisés est purement locale.
- RSVP, déjà cité.
- La virtualisation de réseaux, qui permet de créer un domaine local au-dessus de réseaux physiques divers. Idem pour celle dans les centres de données (RFC 8151).
- Le SFC du RFC 7665, qui permet d'attacher des instructions particulières aux paquets (encodées selon le RFC 8300), instructions qui n'ont évidemment de sens que dans un domaine local.
- Dans un genre analogue, il y a aussi le routage par les segments (RFC 8402).
- L'IETF a une série d'adaptations des protocoles Internet spécialement conçues pour le cas de la maison, collectivement nommées Homenet (RFC 7368, RFC 7788).
- Avec IPv6, d'autres possibilités amusantes existent. L'étiquette de flot (RFC 6294) peut permettre de marquer tel ou tel flot de données, pour ensuite lui appliquer une politique spécifique. Les en-têtes d'extension permettent de déployer des techniques comme le routage via des segments, cité plus haut. (Le fait que ces en-têtes passent mal sur l'Internet public - cf. RFC 7045 et RFC 7872 n'est pas un problème dans un domaine limité.) Et la grande taille des adresses IPv6 permet d'encoder dans l'adresse des informations qui seront ensuite utilisées par les machines du domaine.
- Et enfin je vais citer les PvD ("*ProVisioning Domain*") du RFC 7556, qui formalisent cette notion de domaine local, et lui donnent un cadre.

La section 5 du RFC conclut qu'il peut être souhaitable d'avoir des protocoles explicitement réservés à des domaines limités, et pour qui les règles pourraient être différentes de celles des protocoles conçus pour le grand Internet ouvert. Le RFC donne un exemple : si faire ajouter des en-têtes d'extension à un paquet IPv6 par le réseau qu'il traverse serait une abominable violation de la neutralité `<https://www.bortzmeyer.org/neutralite.html>`, en revanche, dans un domaine local, pourquoi ne pas se dire que ce serait possible, et peut-être intéressant dans certains cas ? Pour de tels protocoles, on ne pourrait pas garantir leur interopérabilité sur l'Internet, mais ils pourraient former une intéressante addition au socle de base du travail de l'IETF, qui sont les protocoles de l'Internet public.

Une fois posée l'opinion que les protocoles « à usage local » sont intéressants (et qu'ils existent déjà), comment les améliorer ? Actuellement, comme le concept de « domaine limité » n'est pas explicitement défini, le domaine est créé par la configuration des machines, des pare-feux, des résolveurs DNS, des ACL, du VPN…Un processus compliqué et où il est facile de se tromper, surtout avec le BYOD, le télétravail…Imaginez un serveur HTTP privé, qui ne sert que le domaine. Comment le configurer pour cela ? Compter sur les pare-feux ? Mettre des ACL sur le serveur (ce qui nécessite de connaître la liste, évolutive, des préfixes IP du domaine) ? Définir un domaine nécessite d'avoir un intérieur et un extérieur, et que chaque machine, chaque application, sache bien de quel côté elle est (ou à l'interface entre les deux, si elle sert de garde-frontière). Et, quand on est à l'intérieur, et qu'on envoie ou reçoit un message, il est important de savoir si on l'envoie à l'extérieur ou pas, si on le reçoit de l'intérieur ou pas. Bref, actuellement, il n'y a pas de solution propre permettant de répondre à cette question.

Le RFC définit alors un cahier des charges pour qu'on puisse définir des règles locales et que ça marche. Notamment :

— Comme tout truc sur l'Internet, le domaine devrait avoir un identificateur. Le RFC suggère que ce soit une clé publique cryptographique, pour permettre les authentifications ultérieures. (Le RFC 7556, sur les PvD, propose plutôt que ce soit un simple FQDN.)
— Il serait bien sympa de pouvoir emboîter les domaines (un domaine limité dans un autre domaine limité).
— Les machines devraient pouvoir être dans plusieurs domaines.
— Idéalement, les machines devraient pouvoir être informées des domaines qu'elles peuvent rejoindre, pour pouvoir choisir.
— Évidemment, tout cela devrait être sécurisé. (Par exemple avec un mécanisme d'authentification de la machine.)
— Il faudrait un mécanisme de retrait. (Une machine quitte le domaine.)
— Ce serait bien de pouvoir savoir facilement si telle machine avec qui on envisage de communiquer est dans le même domaine que nous.
— Et enfin on voudrait pouvoir accéder facilement aux informations sur la politique du domaine, par exemple sur ses règles de filtrage. (Exemple : un domaine limité de l'employeur interdisant de contacter tel ou tel service.)

À l'heure actuelle, tout ceci relève du vœu pieux.

Une motivation fréquente des domaines locaux (ou limités) est la sécurité. La section 7 de notre RFC, dédiée à ce sujet, fait remarquer qu'on voit souvent des gens qui croient que, dans un domaine limité, on peut réduire la sécurité car « on est entre nous ». Cela oublie, non seulement le fait que la plupart des menaces sont internes (par une malhonnêteté ou par une infection), mais aussi celui qu'un protocole qu'on croyait purement interne se retrouve parfois utilisé en extérieur. Un exemple classique est le site Web « interne » pour lequel on se dit que HTTPS n'est pas nécessaire. Si, suite à un problème de routage ou de pare-feu, il se retrouve exposé à l'extérieur, il n'y aura pas de seconde chance.

Enfin, l'annexe B du RFC propose une taxonomie des domaines limités : utile si vous voulez creuser la question.