

afnic

Les RFC, c'est quoi et comment sont-ils faits ?

Stéphane Bortzmeyer

`<bortzmeyer@nic.fr>`

afnic

1 / 42

afnic

2 / 42

L'AFNIC

L'AFNIC - Association Française pour le Nommage Internet en Coopération - est le registre des noms de domaine en .fr.
L'AFNIC, association à but non lucratif, reverse 90 % de ses bénéfices à sa Fondation pour la solidarité numérique.

<https://www.afnic.fr/>

afnic

3 / 42

Plan de l'intervention

- 1 Les RFC
- 2 Les SDO
- 3 Normes et gouvernance
- 4 Participer

afnic

4 / 42

Que sont les RFC ?

- RFC voulait dire autrefois « *Request For Comments* »,
- Aujourd'hui, c'est une série de textes très variés au sujet de l'Internet,
- Qui inclut notamment les normes techniques de l'Internet (« TCP/IP »).

Importance des protocoles

- Tout l'Internet fonctionne grâce à des **protocoles**,
- Un protocole est un ensemble de règles que doivent suivre les deux machines,
- Il permet l'**interopérabilité**,
- Idéalement, un protocole est décrit dans une **spécification**, le texte qui énonce les règles.

C'est quoi, une norme ?

- Une spécification écrite par une organisation de normalisation,
- Stable, archivée, disponible (mais pas toujours).

Quelques exemples de RFC

- RFC 7230 et suivants : la norme HTTP,
- RFC 4271 : la norme BGP (*Border Gateway Protocol*), le protocole d'infrastructure de routage,
- RFC 8484 : la norme DoH (DNS sur HTTPS),
- RFC 5198 : la norme pour le texte brut en Unicode,
- RFC 3339 : format des dates (profil - restriction - de ISO 8601),
- RFC 8897 : le dernier paru, le 3 septembre 2020 (sur un aspect de la RPKI, technique de sécurisation du routage BGP).

Statut d'un RFC

- Tous les RFC ne sont pas des normes,
- Ils peuvent également être « pour information » (exemple : RFC 7626 décrivant les vulnérabilités du DNS sur les questions de vie privée),
- Ou « expérimental » (exemple : RFC 6126 décrivant le protocole de routage Babel, pour les réseaux non-gérés).

Le RFC Editor

- Les RFC sont publiés, archivés et distribués par une organisation spéciale, le *RFC Editor*,
- <https://www.rfc-editor.org/>,
- Archiver sur le long terme n'est pas facile dans le monde numérique (le RFC 768, norme d'UDP, date de 1980, avant IPv4 !)

Un RFC pris au hasard



RFC 8020

NXDOMAIN: There Really Is Nothing Underneath, NOVEMBER 2016

File formats:

  

Status:
PROPOSED STANDARD

Updates:
RFC 1034, RFC 2308

Authors:
S. Bortzmeyer
S. Huque

Stream:
IETF



11 / 42

Autre choses à savoir

- Uniquement en anglais,
- Autrefois forcément en texte seul, et ASCII (mais ça vient de changer),
- Documents très techniques, non prévus pour le grand public.

Extrait du RFC 8020

When an iterative caching DNS resolver receives an NXDOMAIN response, it SHOULD store it in its cache and then all names and resource record sets (RRsets) at or below that node SHOULD be considered unreachable. Subsequent queries for such names SHOULD elicit an NXDOMAIN response.

Les autres normes techniques

- Les RFC vont de la « couche 3 » (Réseau) au bas de la « couche 7 » (Applications),
- On trouve beaucoup d'autres normes techniques : 5G, Wi-Fi ou CSS ne sont pas dans des RFC.

Plan de l'intervention

- 1 Les RFC
- 2 Les SDO
- 3 Normes et gouvernance
- 4 Participer

Qui produit les normes ?

- Les SDO (*Standards Developing Organization*),
- Il n'y a pas **une** SDO officielle,
- La plupart des SDO sont des organisations privées, souvent sans statut officiel,
- Une SDO n'est pas la police, elle n'a pas le pouvoir de contraindre à utiliser ses normes.

Exemples de SDO

- IETF (la plupart des RFC),
- W3C (HTML, CSS, API JavaScript, ActivityPub...),
- IEEE (couches 1 et 2),
- Consortium Unicode (jeu de caractères universel),
- UIT (plus grand'chose sur l'Internet, à part X.509),
- Les SDO se différencient par la disponibilité de leurs normes, l'ouverture de la participation, la transparence des processus...

L'IETF

- *Internet Engineering Task Force*,
- <https://www.ietf.org/>,
- Ouverte à tous et toutes, pas de conditions d'inscription,
- Tout est fait en public (en théorie), archivé et disponible.

Comment travaille l'IETF

- Listes de diffusion,
- Outils de travail en groupe (DataTracker pour suivre les documents, MailArchive pour les courriers),
- De plus en plus de GitHub (hélas),
- Des réunions physiques trois fois par an (mais, ça, c'était avant),
- Des hackathons.

Le DataTracker

The screenshot shows the DataTracker interface for the document 'draft-ietf-drip-arch'. The browser address bar shows the URL 'https://datatracker.ietf.org/doc/draft-ietf-drip-arch/'. The page title is 'Drone Remote Identification Protocol (DRIP) Architecture' with the identifier 'draft-ietf-drip-arch-03'. There are tabs for 'Status', 'IESG evaluation record', 'IESG writeups', 'Email expansions', and 'History'. A 'Versions' section shows a timeline from February 2020 to July 2020 with version numbers 00, 01, 02, and 03. The document details include: Type: Active Internet-Draft (drip WG); Last updated: 2020-07-13; Replaces: draft-card-drip-arch; Stream: IETF; Intended RFC status: (None); Formats: plain text, html, xml, pdf, htmlized (tools), htmlized, bibtex; WG state: WG Document (wg milestones: May 2020 - Requirements and arc..., Jul 2020 - Requirements and arc...); Document shepherd: No shepherd assigned; IESG state: I-D Exists; Consensus: Unknown; Boilerplate; Telechat date.

La prise de décision

- Pas de vote,
- « Consensus approximatif »,
- Les liens personnels comptent.

Organisation de l'IETF

- Divisée en zones (*areas*) elles-mêmes découpées en groupes de travail (WG, *Working Group*),
- Exemples de zones : Routage, Transport (« couche 4 »)...
- Exemples de groupes : dans Applications, le groupe capport (portails captifs), dans Transport, le groupe quic, dans Routage, le groupe babel...
- La direction technique est assurée par l'IESG (*Internet Engineering Steering Group*),
- La réflexion à plus long terme par l'IAB (*Internet Architecture Board*).

Organisation administrative de l'IETF

- La structure légale est l'IETF LLC,
- Avec l'appui et le financement de l'ISOC (*Internet Society*).

La naissance d'un RFC

- Il existe de nombreux parcours possibles pour un RFC,
- Prenons comme exemple une norme,
- Ayant un parcours assez typique (mais il y a beaucoup de variations possibles).

Parcours d'une norme

- Des personnes ont une idée,
- Rédigent un *Internet-Draft* (pas de limitation, tout le monde peut en rédiger et l'IETF les publie),
- Sur cette base, ces personnes discutent avec d'autres participants IETF,
- Et cela débouche sur une proposition de groupe de travail,
- Si l'IESG l'accepte, le groupe est créé,
- Le groupe travaille sur l'idée, l'*Internet-Draft* passe par plusieurs itérations.

Parcours d'une norme, suite et fin

- Après un dernier appel dans le groupe, envoi à l'IESG,
- Après approbation par l'IESG, envoi au *RFC Editor*,
- Le RFC est publié.

Exemples de parcours

- Le protocole QUIC
 - Nait d'une proposition Google (du même nom),
 - Discussions à l'IETF en juin 2016,
 - Groupe de travail créé en octobre 2016,
 - RFC pas encore approuvés (en *WG Last Call*).
- Le protocole DoH
 - Discussions en mai-septembre 2017,
 - Groupe créé presque tout de suite,
 - RFC publié en octobre 2018.
- RFC 8773 (extension à TLS)
 - Premier projet en mars 2018,
 - Adopté par le groupe de travail tls en février 2019,
 - RFC publié en mars 2020.

Des RFC surprenants

- Chaque année, au premier avril, un ou plusieurs RFC d'humour et qui font parfois réfléchir,
- RFC 8774 : l'intrication quantique permet de la communication instantanée, si un programme divise par la latence, cela fera une division par zéro,
- RFC 8369 : remplacer les adresses IP par des caractères Unicode et avoir donc des émojis à la place des adresses,
- Et le très connu RFC 1149, IP sur pigeons voyageurs.

Plan de l'intervention

- 1 Les RFC
- 2 Les SDO
- 3 Normes et gouvernance
- 4 Participer

Il n'y a pas que la normalisation

- Attention, tout ne se décide pas uniquement via la normalisation formelle,
- L'Internet est « sans permission », tout le monde peut spécifier un protocole et le mettre en œuvre,
- C'est bien ainsi que le Web est né !
- Autre exemple, BitTorrent.
- L'IETF n'a aucun pouvoir ici,
- Elle ne peut pas, ni ne veut, empêcher ces déploiements.

Et le déploiement ?

- Ce n'est pas l'IETF qui décide si une norme sera un succès ou pas,
- Une norme peut ne rencontrer aucun succès,
- Le déploiement ou non-déploiement dépend de beaucoup d'acteurs (FAI, auteurs de logiciels, États...),
- RFC 5218, analyse de succès et d'échecs de divers protocoles,
- Beaucoup de choix ne sont pas dans la norme (exemple des résolveurs par défaut dans DoH).

Controverses, DoH

- DNS sur HTTPS, pour joindre un résolveur distant de manière sécurisée,
- Déplace le pouvoir du FAI vers l'opérateur du résolveur → les FAI ne sont pas ravis,
- Empêche certaines formes de censure → les censeurs ne sont pas ravis,
- Débat confus (DoT permettait la même chose mais n'a pas fait l'objet de débats).

Controverses, DoH, suite

- Certains choix de déploiement (résolveur Cloudflare par défaut) ne sont pas liés à DoH mais à une mise en œuvre (Mozilla Firefox),
- Tout le monde prétend défendre « les utilisateurs ».

Controverses, TLS 1.3

- La version 1.3 de ce protocole de sécurité résout quelques failles qui permettaient la surveillance,
- Ceux qui exploitaient ces failles sont mécontents,
- Demande de « visibilité » (casser la confidentialité).

RFC plus politiques

- Disons que l'IETF a une autorité morale,
- Plusieurs RFC sont de nature politique et décrivent ce que l'IETF considère comme juste,
 - RFC 1984, refus d'affaiblir la cryptographie,
 - RFC 6973, sur l'importance de la vie privée,
 - RFC 7258, déclarant que la surveillance massive est une attaque,
 - RFC 8280, Internet et droits humains,
 - RFC 8890, priorité aux utilisateurs.

Plan de l'intervention

- 1 Les RFC
- 2 Les SDO
- 3 Normes et gouvernance
- 4 Participer

Pourquoi participer

- La normalisation technique n'est pas tout, mais elle est très importante,
- Les normes définissent ce qui va être facile et ce qui va être difficile à faire,
- Exemple du chiffrage : en l'absence de chiffrage systématique, la surveillance est facile.

Tensions

- Différents groupes et différentes personnes ont des intérêts et des opinions différents,
- Si un seul groupe fait la normalisation, les normes ne refléteront que ses choix,
- D'où l'importance d'une participation large.

Quelques pré-requis à la participation

- L'anglais, et la technique,
- Et du temps disponible,
- L'argent est beaucoup moins un problème,
- Savoir programmer aide (l'IETF valorise le concret) mais n'est pas obligatoire,
- Les discussions sont franches ou ouvertes, et en public,
- Globalement beaucoup moins de barrières que dans d'autres SDO.

Comment participer

- (Vous pouvez aussi profiter du travail fait par d'autres, des **médiateurs**, par exemple à l'ISOC.)
- Y aller progressivement,
- Commencer par lire des RFC et des *Internet-Drafts*,
- Puis les discussions sur les listes de diffusion des groupes de travail,
- Se lancer : commenter des *Internet-Drafts*, en écrire.

Comment participer, suite

- Nombreuses ressources pour les débutants
<https://www.ietf.org/about/participate/>.
- Dans tous les cas, ne soyez pas seul : par exemple, profitez des *hubs* créés dans certains pays pour permettre une participation à distance et collective aux réunions.

Exemple : hackathon distant depuis Maurice

