RFC 6335 : Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Transport Protocol Port Number and Service Name Registry

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 3 septembre 2011

Date de publication du RFC : Août 2011

https://www.bortzmeyer.org/6335.html

Ce RFC parle autant de gouvernance que de technique. Il refond considérablement les procédures utilisées pour enregistrer les numéros de port à l'IANA. Bien que moins médiatisé que l'enregistrement des noms de domaine, ou même que celui des adresses IP, cet enregistrement des ports a déjà suscité des conflits, et peut en faire encore plus maintenant qu'une des plages utilisées approche de la saturation. L'ancien mécanisme d'enregistrement était peu documenté, avait plusieurs limites techniques, et était éclaté entre plusieurs registres ayant des règles différentes. Le nouveau vise à unifier tout cela et à suivre de bons principes, soigneusement explicités.

D'abord, de quoi s'agit-il (section 3) ? Les ports sont des numéros, codés sur 16 bits, qui servent à démultiplexer les paquets IP entrant dans une machine (port de destination 62981 -¿ processus 7653, qui fait tourner dig, etc) et à identifier le protocole utilisé (port 80 -¿ HTTP, port 22 -¿ SSH, etc). Les noms de services, eux, sont des courts identificateurs alphabétiques, qui servent à s'abstraire du numéro de port, en permettant aux applications d'utiliser un nom de service pour récupérer dynamiquement un numéro de port (par exemple avec les enregistrements SRV du DNS, ou bien avec un appel à `getservbyname()`). Sur Unix, vous avez une liste (incomplète) de ces noms, avec le numéro de port correspondant, dans le fichier `/etc/services`. Pendant longtemps, les registres officiels stockaient à la fois un nom de service et un numéro de port. Désormais, ils pourront ne contenir qu'un nom de service.

Le port n'est pas indiqué dans l'en-tête IP mais dans celle du protocole de couche 4 au dessus. On peut donc techniquement utiliser le même numéro de port pour des applications différentes, si l'une utilise UDP et l'autre TCP. La procédure d'enregistrement, elle, est désormais la même pour tous les protocoles de transport.

Les en-têtes de couche 4 incluent deux ports, celui de source et celui de destination, et, avec les adresses IP source et destination et l'identificateur du protocole de transport, ils servent aussi à identifier une connexion de manière unique.

Du fait que l'ancien système d'enregistrement à l'IANA allouait en même temps un nom de service et un numéro de port, bien des applications savent utiliser ce nom de service. Par exemple, avec telnet, on peut se connecter à un serveur de courrier avec `telnet mail.example.net 25` (le numéro de port) mais aussi avec `telnet mail.example.net smtp` (le nom du service). Le port ainsi enregistré est dit « bien connu » (80 pour HTTP...) Mais attention : de nos jours, il est courant de faire tourner une application sur un port autre que celui prévu à l'origine (parce que le pare-feu ne laisse passer que le port 80, pour échapper à la détection, ou encore parce qu'on veut faire tourner deux mises en œuvre différentes du protocole sur la même machine, ou derrière le même routeur NAT). Enfin, certaines applications n'ont pas de port fixe et comptent sur les enregistrements SRV du DNS (RFC 2782 [1]), ou bien sur d'autres méthodes (comme les "*trackers*" dans BitTorrent).

Un dernier points sur les numéros de port : comme ils sont stockés sur seulement 16 bits, il n'y a que 65 536 valeurs possibles. C'est très peu. La première plage, celle des ports bien connus, est déjà pleine à 76 %. Un des objectifs de la politique d'allocation des ports est donc d'épargner cette ressource limitée, notamment en conseillant fortement aux applications d'utiliser uniquement un nom de service, sans réserver de numéro de port.

Le plan du RFC commence par expliquer la situation actuelle et pourquoi elle n'est pas satisfaisante. Mais je préfère partir de la nouvelle situation, celle qui est désormais l'officielle, et parler du passé tout à la fin de cet article.

D'abord, les noms de services (section 5). Ce sont les clés d'accès au registre des services <`https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml`>. Les applications les utilisent pour chercher un numéro de port, typiquement via les enregistrements SRV du RFC 2782. Il peut y avoir plusieurs services qui se partagent un numéro de port, par exemple :

— Parce que l'un est une extension de l'autre (cas de TURN - RFC 8656, qui est une extension de STUN - RFC 8489 ; le fait d'avoir un service nommé `turn` permet à une application d'obtenir tout de suite un serveur ayant l'extension TURN, sans tester plusieurs serveurs STUN),
— Par accident (un exemple typique est la coexistence de deux services `www` et `http` qui pointent vers le même port 80 ; seul `http` est correct, aujourd'hui),
— Ou suite à la sortie de notre RFC qui introduisait des nouvelles règles de syntaxe pour les noms de services, rendant parfois nécessaire la création d'alias (l'ancien et le nouveau nom).

Les noms de services dans le registre <`https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml`> sont enregistrés sur une base « premier arrivé, premier servi », tel que décrit dans le RFC 5226 (voir aussi la section 7.2). Contrairement aux numéros de port, il n'y a pas de pénurie et donc pas de raison de faire des économies, sauf si l'IANA détecte un problème (comme un enregistrement massif de noms) auquel cas elle peut passer au mécanisme "*Expert review*", où un examen de fond est fait. Les noms doivent être courts (quinze caractères maximum) et informatifs, et éviter les redondances (comme de mettre protocole ou port dans le nom).

La syntaxe des noms (une nouveauté de ce RFC) est décrite en section 5.1. En résumé, seuls les lettres d'ASCII, les chiffres et le tiret sont admis. Il faut au moins une lettre, pour éviter des noms de service comme 23, qui pourrait être pris pour un numéro de port. 98 % des noms du registre étaient

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2782.txt`

déjà conformes à cette syntaxe avant ce RFC, les 2 % restants ont dû changer de nom pour se plier à la nouvelle syntaxe. C'est ainsi que, par exemple, `z39.50` (pour le protocole du même nom) est devenu `z39-50`.

Dans le cas le plus courant, l'application va traduire ces noms en numéro de port via une requête DNS. Prenons l'exemple de XMPP. Si le serveur de messagerie instantanée de Google Talk veut contacter un utilisateur dont l'adresse XMPP est `martinedurand@dns-oarc.net`, le serveur de Google va faire une requête SRV pour le service `xmpp-server`, protocole TCP (RFC 6120, section 3.2.1). Il trouvera :

```
% dig SRV _xmpp-server._tcp.dns-oarc.net
...
;; ANSWER SECTION:
_xmpp-server._tcp.dns-oarc.net. 3600 IN SRV 0 0 5269 jabber.dns-oarc.net.
```

et saura donc qu'il doit se connecter au port 5269. (Le fait que le champ « service » du RFC 2782 doive être un nom de service enregistré n'était pas clair : c'est notre nouveau RFC qui impose cette règle.)

L'enregistrements des numéros de port est plus complexe, en raison du risque de pénurie (section 6). Il y a trois plages de numéros de port :

— Les ports « système », dits aussi « bien connus », de 0 à 1023.
— Les ports « utilisateur », de 1024 à 49151.
— Et les ports « dynamiques », dits aussi « éphémères », de 49152 à 65535. Contrairement aux deux précédentes plages, ils ne font jamais l'objet d'un enregistrement à l'IANA.

Il y a trois statuts possibles pour un numéro de port :

— Affecté : il apparaît alors dans le registre <https://www.iana.org/assignments/service-names-port-nu
service-names-port-numbers.xml>,
— Non affecté,
— Réservé : ils ne sont pas affectés et ne doivent normalement pas l'être. Par exemple, les ports extrêmes de la plage des bien connus, 0 et 1023, sont réservés, au cas où il faille un jour étendre cette plage ; on les utiliserait alors comme indiquant un échappement.

Aujourd'hui, 76 % des ports système et 9 % des ports utilisateur sont affectés.

Il existe aussi des ports voués à des usages expérimentaux (section 6.1, voir aussi le RFC 3692), les ports 1021 et 1022. Comme des tas de protocoles peuvent s'y bousculer, les applications qui utilisent ces ports doivent s'assurer qu'elles se connectent bien au service attendu (par exemple, le client peut vérifier que le serveur envoie un nombre magique caractéristique de l'application).

Comment enregistre-t-on un nouveau numéro de port ? La section 7 décrit les grands principes. Le plus important est la nécessité d'allouer lentement, pour éviter d'épuiser ce qui reste de cette ressource (si vous développez un nouveau protocole, rappelez-vous que la méthode recommandée est de ne pas réclamer de numéro de port du tout, mais d'utiliser un nom de service). Environ 400 ports par an sont affectés, et le chiffre est stable depuis des années. Cela devrait permettre de tenir jusqu'à la fin du 21ème siècle.

Compte-tenu de cela, les nouveaux principes, exposés en section 7.2 sont :

— Un seul numéro de port par application : si celle-ci est composée de plusieurs services, l'application doit néanmoins tout mettre sur le même numéro de port et démultiplexer elle-même.
— Même chose en cas de mise à jour d'un service : on n'alloue pas de nouveau numéro de port. La technique recommandée est que le service inclue un champ Version dans ses messages, pour qu'il puisse les séparer facilement.

— Affectation uniquement pour le protocole de transport indiqué (c'est une grande nouveauté par rapport aux précédentes règles). Si l'application ne fonctionne que sur TCP, aucune allocation de port n'est faite pour UDP.
— Rien n'est éternel et une allocation de numéro de port peut être reprise par l'IANA.

Les ports « repris » auront le statut Réservé (sur l'Internet, il n'est pas prudent de réallouer des ports trop tôt, on ne peut jamais être sûr de ce qui traîne dans des vieilles applications, cf. section 8.3). Le jour où une plage de numéros de port est épuisée, l'IANA pourra recycler ces vieux numéros en les affectant.

Tout le détail des procédures bureaucratiques est en section 8. Si on veut un numéro de port ou un nom de service, il faut remplir un formulaire (section 8.1.1) indiquant les coordonnées du demandeur (pour les normes au sens propre, ce demandeur sera l'IETF), une description du protocole prévu et le nom du protocole de transport (TCP, UDP, etc). Si on veut un numéro de port, on peut préciser lequel (et l'IANA le donnera, sauf bonne raison contraire). Les ports rigolos comme 42, 666 ou 1984 (utilisé par un logiciel de surveillance) sont déjà pris.

Rappelez-vous qu'il y aura une grosse différence entre demande d'un numéro de port et demande d'un simple nom de service. Les premiers feront l'objet d'une "*Expert Review*" (cf. RFC 5226), le seconds seront distribués sans trop de formalité. Pour les numéros de port, cela dépendra en outre de la plage visée. La plage dynamique ne permet pas de réservation du tout, la plage utilisateur est recommandée pour les nouvelles réservations, la plage système, celle des ports bien connus, est tellement pleine que l'enregistrement est découragé, un avis d'expert ne suffira pas, il faudra un "*IETF review*" et encore, après avoir expliqué en détail pourquoi ne pas utiliser un port de la plage utilisateur.

Nouveauté de notre RFC, il y a désormais des procédures explicites pour le retrait d'un enregistrement (section 8.2 ; cela concerne surtout les numéros de port, les noms de service peuvent rester enregistrés sans que cela ne gène personne). Le demandeur original peut demander un retrait, s'il n'a plus besoin de l'enregistrement. Mais l'IANA peut aussi le faire d'autorité, si cela semble vraiment nécessaire.

Dans tous les cas, l'IANA tentera de déterminer si le port est encore utilisé.

En revanche, le transfert d'un enregistrement (numéro de port ou nom de service) d'un protocole à un autre est formellement interdit (section 8.4), même entre adultes consentants. Pas de marché des numéros de port, qui aurait permis à ceux qui avaient déposé des numéros il y a longtemps de gagner de l'argent en les vendant maintenant qu'ils sont rares. Si on veut récupérer un numéro de port, il faut le faire désaffecter, puis candidater pour l'avoir.

Il y aura sans doute des désaccords et des crises (comme dans l'affaire CARP <`http://kerneltrap.org/node/2873`>). La procédure habituelle de gestion des conlits à l'IETF (section 7 du RFC 5226) sera donc utilisée.

Un peu d'histoire, maintenant. Quels étaient les procédures avant notre RFC ? Les règles IANA étaient dans le RFC 2780 et notre RFC remplace ses sections 8 et 9. Il y avait aussi des règles spécifiques aux différents protocoles de transport : RFC 3828 pour UDP-Lite, RFC 4340 pour DCCP, et RFC 4960 pour SCTP. Mais elles n'étaient pas complètes (une partie de la procédure était également dans les formulaires Web de soumission à l'IANA, une autre partie était dans le texte du registre), et aussi bien l'IANA que ses « clients » se plaignaient de leur flou (section 1). La section 7.1 de notre RFC 6335 tente de résumer a posteriori les règles (largement informelles) qui étaient utilisées (affectation du port pour TCP et UDP simultanément, pas d'enregistrement des noms de service séparément des ports, SCTP et DCCP traités à part, etc).

En outre, les enregistrements SRV du RFC 2782 ajoutaient leurs propres concepts (nom de service, notion mal définie dans le RFC 2782) et leur propre registre. Ainsi, comme les procédures de l'IANA ne permettaient pas d'enregistrer un nom de service sans obtenir en même temps un numéro de port, on a vu apparaître un registre informel <http://www.dns-sd.org/ServiceTypes.html> des noms de service (qui a fusionné avec l'officiel, cf. section 10). Un des changements importants de ce RFC 6335 est d'unifier les procédures d'enregistrement et les registres.

La syntaxe admissible pour les noms de service n'avait même jamais été spécifiée (section 2). Les formulaires de l'IANA donnaient une limite de longueur (arbitraire et, d'ailleurs, pas toujours respectée dans le registre) à 14 caractères, mais sans préciser si des caractères comme le + ou le / étaient autorisés. On trouvait donc des noms avec des caractères non-alphanumériques comme `whois++` (RFC 2957) ou `sql*net`.

D'autre part, il n'existait aucune procédure écrite pour les opérations postérieures à l'enregistrement : changement, ou suppression (volontaire ou forcée).

PS : si vous vous intéressez aux questions d'enregistrement de paramètres pour les protocoles, voyez la nouvelle liste de discussion happiana <http://www.ietf.org/mail-archive/web/happiana/current/msg00000.html>.