

RFC 791 : Internet Protocol

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 Septembre 2006. Dernière mise à jour le 18
Février 2008

Date de publication du RFC : Septembre 1981

<http://www.bortzmeyer.org/791.html>

Vingt-cinq ans ce mois-ci, un quart de siècle que le protocole IP, dans sa version 4, sert de soubassement à tout l'Internet.

Voici donc le RFC, écrit par Jon Postel lui-même, qui décrit IP. Ses concepts, le routage, l'adressage, le format de paquets.

Le RFC explique très clairement la place d'IP : il ne fournit presque aucun service « de bout en bout », il se content d'acheminer des datagrammes.

L'adressage est traité en quelques paragraphes, CIDR n'existait pas encore, et notre RFC parle donc de « classes » d'adresses, qui seront supprimées en 1993. Le routage est décrit très succinctement.

Le format des paquets (section 3.1) occupe finalement l'essentiel du RFC mais la section 3.2, consacrée à la discussion des détails du protocole, est très instructive, notamment sur la difficile question de la fragmentation des paquets.

Il n'existe pas de langage standard pour décrire un format de paquets donc notre RFC, comme tous les autres, utilise dans sa section 3.1, de l'art ASCII. Voici l'en-tête d'un paquet IP :

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+
|Version|  IHL  |Type of Service|      Total Length      |
+-----+-----+-----+-----+
|      Identification      |Flags|      Fragment Offset  |
+-----+-----+-----+-----+
| Time to Live | Protocol |      Header Checksum      |
+-----+-----+-----+-----+
|      Source Address      |
+-----+-----+-----+-----+
|      Destination Address |
+-----+-----+-----+-----+
|      Options      |      Padding      |
+-----+-----+-----+-----+
```

La version vaut toujours 4 pour IPv4. Beaucoup de décodeurs comme tcpdump affichent simplement « IP » tout court, lorsqu'il s'agit d'IPv4. Voici ce qu'affiche tcpdump avec l'option `-vvv` :

```
21:59:43.111985 IP (tos 0x8, ttl 64, id 16854, offset 0, flags [DF], length: 60) 172.19.1.1.35890 > 172.19.1.2
```

Le ToS ("*Type of Service*", voir plus loin) vaut ici 8 (en hexadécimal), le TTL ("*Time to Live*", en dépit de son nom, c'est le nombre maximum de routeurs qu'on peut traverser avant que le paquet ne soit abandonné) vaut 64, l'identificateur du fragment vaut ici 16854 et l'option ("*flag*") DF ("*Don't Fragment*") est à « vrai » (c'est la découverte de MTU du RFC 1191¹). Attention, l'ordre d'affichage n'est pas celui du paquet.

tshark, donne d'avantage de détails que tcpdump, d'une manière qui respecte bien le modèle en couches :

```
# tshark -V -n
...
Frame 1 (74 bytes on wire, 74 bytes captured)
  Arrival Time: Feb 18, 2008 22:04:15.826000000
...
Internet Protocol, Src Addr: 172.19.1.1 (172.19.1.1), Dst Addr: 172.19.1.2 (172.19.1.2)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x08 (DSCP 0x02: Unknown DSCP; ECN: 0x00)
    0000 10.. = Differentiated Services Codepoint: Unknown (0x02)
    .... ..0. = ECN-Capable Transport (ECT): 0
    .... ...0 = ECN-CE: 0
  Total Length: 60
  Identification: 0xeeec (61164)
  Flags: 0x04 (Don't Fragment)
    0... = Reserved bit: Not set
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
  Header checksum: 0xf19d (correct)
  Source: 172.19.1.1 (172.19.1.1)
  Destination: 172.19.1.2 (172.19.1.2)
```

On note que tshark a affiché le champ ToS sous le nom de DSCP, suivant l'évolution qui a eu lieu dans le RFC 2474, qui a complètement changé la sémantique de ce champ et son nom. Normalement, on ne devrait plus parler de ToS, même si ce terme reste fréquent.

Comment changer ce champ ? Un programme comme echoping <<http://echoping.sourceforge.net/>> permet, avec ses options `-p` et `-P`, de donner une valeur à ce champ. Le paquet ci-dessus a été généré par un echoping `-P 0x08 172.19.1.2`.

On notera enfin que c'est ce RFC 791 qui a défini, dans son annexe B, la notion d'ordre des octets sur le réseau. IP est gros boutien, le bit le plus significatif doit être envoyé en premier.

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc1191.txt>