RFC 9774 : Deprecation of AS_SET and AS_CONFED_SET in BGP

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 mai 2025

Date de publication du RFC : Mai 2025

https://www.bortzmeyer.org/9774.html

Dans le protocole de routage BGP, les annonces de routes sont marquées avec l'AS d'origine et avec les AS qui ont relayé l'annonce. Dans ce chemin des AS, on pouvait indiquer un ensemble d'AS, l'AS_SET (ainsi que l'AS_CONFED_SET). C'était déconseillé depuis le RFC 6472[1] et ce nouveau RFC 9774 l'interdit désormais. Le but est de simplifier BGP et notamment ses mécanismes de sécurité. Il faut maintenant forcément indiquer une suite ordonnée d'AS, une AS_SEQUENCE.

Ces AS_SET (et les AS_CONFED_SET du RFC 5065 mais je vais passer rapidement sur les confédérations) sont spécifiés par le RFC 4271, sections 4.3 et 5.1.2. Attention à ne pas confondre avec les objets de type as-set des bases des RIR comme, par exemple, celui de l'Afnic <https://apps.db.ripe.net/db-web-ui/query?bflag=false&dflag=false&rflag=true&searchtext=AS-AFNIC&source=RIPE>.

Un des inconvénients de ces AS_SET est que, puisqu'un ensemble n'est pas ordonné, il n'est pas évident de déterminer l'AS d'origine, le premier AS, ce qui est pourtant nécessaire pour la sécurité (ROV ou "*Route Origin Validation*", cf. RFC 6811).

Pourquoi mettait-on des AS_SET alors ? Parce que c'est utile lorqu'on effectue de l'agrégation de routes. L'agrégation, spécifiée dans les sections 9.1.2.2 et 9.1.4 du RFC 4271 est le mécanisme par lequel un routeur rassemble plusieurs routes en une route plus générale. Si les routes originales venaient de plusieurs AS, on pouvait les rassembler en un AS_SET. Mais, évidemment, cela brouille l'information sur la vraie origine d'une route. C'est pour cela que les techniques de sécurisation de BGP, comme le BGPsec du RFC 8205 ne s'entendent pas bien avec les AS_SET.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6472.txt

La section 3 est la partie normative du RFC : désormais, une machine qui parle BGP ne doit plus utiliser d'AS_SET ou d'AS_CONFED_SET dans les chemins d'AS de ses messages de mise à jour de routes. Une machine qui reçoit ce genre de messages doit les traiter comme une erreur et retirer les routes (cf. RFC 7606). Les techniques de sécurisation comme ROV (RFC 6811) ou BGPsec (RFC 8205) considèrent toute annonce incluant des AS_SET comme invalide.

Sur l'agrégation, voyez par exemple cette réponse sur StackExchange <https://networkengineering.stackexchange.com/a/14953>. La procédure désormais suggérée pour en faire (section 5) est d'indiquer comme AS d'orgine du préfixe agrégé l'AS qui a fait l'agrégation (en s'assurant bien qu'il y a un ROA - RFC 6482). Les annexes A et B donnent des exemples détaillés.

Il est frappant de constater que la majorité des documentations BGP des routeurs continue à mettre AS_SET et AS_SEQUENCE sur un pied d'égalité, alors que le RFC 6472 date de déjà 14 ans.

Le RFC note que les AS_SET sont peu utilisés <https://github.com/ksriram25/IETF/blob/main/Detailed-AS_SET-analysis.txt>, et parfois mal (un AS_SET ne comportant qu'un seul AS, ou bien ayant des numéros d'AS spéciaux <https://www.iana.org/assignments/iana-as-numbers-speci iana-as-numbers-special-registry.xml>...). Cherchons un peu. Je prends une RIB ("*Routing Information Base*") complète sur RouteViews <https://routeviews.org/>. Elle est au format MRT ("*Multi-Threaded Routing Toolkit*", RFC 6396). Passons là à travers bgpdump <https://github.com/RIPE-NCC/bgpdump>, produisant un fichier texte. Comment trouver les AS_SET ? J'ai simplement lu le code source de bgpdump :

```
if (space)
    {
      if (segment->type == AS_SET
   || segment->type == AS_CONFED_SET)
 as->str[pos++] = ',';
      else
 as->str[pos++] = ' ';
 }
```

OK, il y a des virgules entre les AS (et une autre partie du code montre que les AS_SET sont placés entre accolades). On peut alors chercher le fichier texte et trouver, par exemple, cette annonce :

```
TIME: 04/16/25 12:00:02
TYPE: TABLE_DUMP_V2/IPV4_UNICAST
PREFIX: 45.158.28.0/23
FROM: 12.0.1.63 AS7018
ORIGINATED: 04/15/25 06:11:28
ASPATH: 7018 3356 3223 {8262,34224} 201200
NEXT_HOP: 12.0.1.63
COMMUNITY: 7018:5000 7018:37232
```

L'annonce du préfixe 45.158.28.0/23, dont l'origine est l'AS 201200, est passée par l'AS 8262 ou bien le 34224, ou bien il y a eu agrégation de deux routes, chacune passée par un de ces deux AS (mais cela n'a pas été marqué). Sur un "*looking glass*", on voit le passage par le 8262 uniquement :

```
Mon Apr 21 10:30:34.855 CEST
BGP routing table entry for 45.158.28.0/23
Paths: (3 available, best #2, not advertised to any peer)
  Path #1: Received by speaker 0
  174 3356 3223 8262 201200, (received-only)
    149.6.34.5 from 149.6.34.5 (38.28.1.70)
      Origin IGP, metric 17060, localpref 100, valid, external
      Community: 174:21100 174:22009
      Origin-AS validity: not-found
      ...
```

Soit ce "*looking glass*" a reçu une autre annonce, soit son code n'affiche que l'un des AS de l'`AS_SET`.

Autre exemple, où l'`AS_SET` est à l'origine :

```
TIME: 04/16/25 12:00:04
TYPE: TABLE_DUMP_V2/IPV4_UNICAST
PREFIX: 67.204.16.0/22
FROM: 89.149.178.10 AS3257
ORIGINATED: 04/10/25 00:44:05
ASPATH: 3257 13876 {15255,396519,396895}
NEXT_HOP: 89.149.178.10
MULTI_EXIT_DISC: 10
AGGREGATOR: AS13876 67.204.31.4
COMMUNITY: 3257:4000 3257:8118 3257:50002 3257:50120 3257:51100 3257:51110
```

Là, il y a eu agrégation, par l'AS 13876, qui a placé un `AS_SET`. Vu par le "*looking glass*" :

```
Mon Apr 21 10:39:46.348 CEST
BGP routing table entry for 67.204.16.0/22
Paths: (3 available, best #2, not advertised to any peer)
  Path #1: Received by speaker 0
  174 3356 13876 {15255,396519,396895}, (aggregated by 13876 67.204.31.4), (received-only)
    149.6.34.5 from 149.6.34.5 (38.28.1.70)
      Origin IGP, metric 17060, localpref 100, valid, external
      Community: 174:21100 174:22009
      Origin-AS validity: not-found
```

Je ne suis pas sûr que tous les "*looking glass*" affichent correctement les `AS_SET`. Mais étant donné que notre nouveau RFC met les `AS_SET` à la poubelle, il ne servirait à rien de demander au développeur d'ajouter ce service. Ah, et mon bot fédivers <`https://www.bortzmeyer.org/fediverse-bot-bgp.html`> qui lit la table BGP gère ça bien <`https://mastodon.gougere.fr/@bgp/114375106512755449`>.