Deprecation of AS_SET and AS_CONFED_SET in BGP
draft-ietf-idr-deprecate-as-set-confed-set-01

Abstract

BCP 172 (i.e., RFC 6472) recommends not using AS_SET and AS_CONFED_SET in the Border Gateway Protocol. This document advances this recommendation to a standards requirement in BGP; it proscribes the use of the AS_SET and AS_CONFED_SET types of path segments in the AS_PATH. This is done to simplify the design and implementation of BGP and to make the semantics of the originator of a route clearer. This will also simplify the design, implementation, and deployment of various BGP security mechanisms. This document (if approved) updates RFC 4271 and RFC 5065 by eliminating AS_SET and AS_CONFED_SET types, and obsoletes RFC 6472.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 1, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents
1. Introduction

BCP 172 [RFC6472] makes a recommendation for not using AS_SET (see [RFC4271]) and AS_CONFED_SET (see [RFC5065]) in the Border Gateway Protocol (BGP). This document advances the BCP recommendation to a standards requirement in BGP; it proscribes the use of the AS_SET and AS_CONFED_SET types of path segments in the AS_PATH.

The AS_SET path segment in the AS_PATH attribute (Sections 4.3 and 5.1.2 of [RFC4271]) is created by a router that is performing route aggregation and contains an unordered set of Autonomous Systems (ASes) that the update has traversed. The AS_CONFED_SET path segment (see [RFC5065]) in the AS_PATH attribute is created by a router that is performing route aggregation and contains an unordered set of Member AS Numbers in the local confederation that the update has traversed. It is very similar to AS_SETs but is used within a confederation.

By performing aggregation, a router is combining multiple existing routes into a single new route. The aggregation together with the use of AS_SET blurs the semantics of origin AS for the prefix being announced. Therefore, the aggregation with AS_SET (or AS_CONFED_SET) can cause operational issues, such as not being able to authenticate a route origin for the aggregate prefix in new BGP security technologies such as those that take advantage of X.509 extensions for IP addresses and AS identifiers [RFC3779] [RFC6480] [RFC6811].
This in turn could result in reachability problems for the aggregated prefix and its components (i.e., more-specific prefixes). The aggregation as described above could also create traffic engineering issues, because the precise path information for the component prefixes are not preserved.

From analysis of past Internet routing data, it is apparent that aggregation that involves AS_SETs is very seldom used in practice on the public Internet [Analysis] and when it is used, it is often used incorrectly -- only a single AS in the AS_SET are by far the most common cases. Also, very often the same AS appears in the AS_SEQUENCE and the AS_SET in the BGP update. The occurrence of reserved AS numbers ([IANA-SP-ASN]) is also somewhat frequent. Because the aggregation involving AS_SETs is very rarely used, the reduction in table size provided by this is extremely small, and any advantage thereof is outweighed by additional complexity in BGP. As noted above, AS_SETs also pose impediments to implementation of new BGP security technologies.

In the past, AS_SET had been used in a few rare cases to allow route aggregation where two or more providers could form the same aggregate prefix, using the exact match of the other’s aggregate prefix in some advertisement and configuring the aggregation differently elsewhere. The key to configuring this correctly was to form the aggregate at the border in the outbound BGP policy and omit prefixes from the AS that the aggregate was being advertised to. The AS_SET therefore allowed this practice without the loss of BGP’s AS_PATH loop protection. This use of AS_SET served a purpose that fell in line with the original intended use. Without the use of AS_SET, aggregates must always contain only less-specific prefixes (not less than or equal to) and must never aggregate an exact match.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Recommendation to Network Operators

Network operators MUST NOT generate any new announcements containing AS_SETs or AS_CONFED_SETs. If they have already announced routes with AS_SETs or AS_CONFED_SETs in them, then they MUST withdraw those routes and re-announce routes for the component prefixes (i.e., the more-specific routes subsumed by the previously aggregated route) without AS_SETs or AS_CONFED_SETs in the updates. A sending router


Kumari, et al. Expires May 1, 2020 [Page 3]
MUST not generate a BGP UPDATE with AS_SET or AS_CONFED_SET. A receiving router MUST treat the announced routes in a BGP UPDATE with AS_SET or AS_CONFED_SET as withdrawn routes.

If a network operator wishes to consider a BGP UPDATE with AS_SET or AS_CONFED_SET for path selection, they MAY have a feature (knob) in the router to opt to do so. The operator should understand the full implications of choosing this option.

Route aggregation that was previously performed by proxy aggregation without the use of AS_SETs is still possible under some conditions. When doing this, operators MUST form the aggregate at the border in the outbound BGP policy and omit any prefixes from the AS that the aggregate is being advertised to. As with any change, the operator should understand the full implications of the change.

It is worth noting that new BGP security technologies (such as those that take advantage of X.509 extensions for IP addresses and AS identifiers [RFC3779] [RFC6480] [RFC6811] [RFC8205]) might not support routes with AS_SETs/AS_CONFED_SETs in them, and may treat routes containing them as infeasible even before the updated BGP in this document is implemented.

4. Updates to Existing RFCs

This document eliminates AS_PATH segment type 1, namely, AS_SET that is specified in Section 4.3 of [RFC4271]. That is, in a future specification of BGP -- one that would obsolete RFC 4271 -- the use of AS_SET will not be specified.

This document also eliminates AS_PATH segment type 4, namely, AS_CONFED_SET that is specified in Section 3 of [RFC5065]. That is, in a future specification of Autonomous System Confederations for BGP -- one that would obsolete RFC 5065 -- the use of AS_CONFED_SET will not be specified.

5. Security Considerations

This document obsoletes the use of aggregation techniques that create AS_SETs or AS_CONFED_SETs. Obsoleting these path segment types from BGP and removal of the related code from implementations would potentially decrease the attack surface for BGP. Deployments of new BGP security technologies [RFC6480] [RFC6811] [RFC8205] benefit greatly if AS_SET and AS_CONFED_SET are not used in BGP.
6. IANA Considerations

This document requires no IANA actions.

7. Acknowledgements

The authors would like to thank Jeffery Haas, John Heasley, Job Snijders, Jared Mauch, Jakob Heitz, Keyur Patel, Douglas Montgomery, Randy Bush, Susan Haes, John Scudder, Curtis Villamizar, Danny McPherson, Chris Morrow, Tom Petch, Ilya Varlashkin, Enke Chen, Tony Li, Florian Weimer, John Leslie, Paul Jakma, Rob Austein, Russ Housley, Sandra Murphy, Steve Bellovin, Steve Kent, Steve Padgett, Alfred Hoenes, and Alvaro Retana for comments and suggestions.

8. References

8.1. Normative References


8.2. Informative References


Authors’ Addresses

Warren Kumari
Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA  94043
US
Phone: +1 571 748 4373
Email: warren@kumari.net

Kotikalapudi Sriram
USA NIST
100 Bureau Drive
Gaithersburg, MD  20899
US
Phone: +1 301 975 3973
Email: sriram.ietf@gmail.com