Workgroup: Network Working Group
Internet-Draft:
draft-wang-idr-flowspec-dip-origin-as-
filter-07
Published: 13 March 2023
Intended Status: Standards Track
Expires: 14 September 2023
Authors: H. Wang A. Wang S. Zhuang
Huawei China Telecom Huawei

Destination-IP-Origin-AS Filter for BGP Flow Specification

Abstract

BGP Flowspec mechanism (BGP-FS) [RFC8955] [RFC8956] propagates both traffic Flow Specifications and Traffic Filtering Actions by making use of the BGP NLRI and the BGP Extended Community encoding formats. This document specifies a new BGP-FS component type to support AS-level filtering. The match field is the origin AS number of the destination IP address that is encoded in the Flowspec NLRI. This function is applied in a single administrative domain.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

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 14 September 2023.

Copyright Notice

Table of Contents

1. Introduction
2. Definitions and Acronyms
3. The Flow Specification Encoding for Destination-IP-Origin-AS Filter
4. Use Cases
5. Security Considerations
6. IANA
7. Contributors
8. Acknowledgments
9. References
Authors' Addresses

1. Introduction

BGP Flow Specification (BGP-FS) [RFC8955] [RFC8956] defines a new BGP NLRI to distribute traffic flow specification rules via BGP ([RFC4271]). BGP-FS policies have a match condition that may be n-tuple match in a policy, and an action that modifies the packet and forwards/drops the packet. Via BGP, new filter rules can be sent to all BGP peers simultaneously without changing router configuration, and the BGP peer can install these routes in the forwarding table. BGP-FS defines Network Layer Reachability Information (NLRI) format used to distribute traffic flow specification rules. NLRI (AFI=1, SAFI=133) is for IPv4 unicast filtering. NLRI (AFI=1, SAFI=134) is for BGP/MPLS VPN filtering.[I-D.ietf-idr-flowspec-l2vpn][I-D.ietf-idr-flowspec-l2vpn] extends the flow-spec rules for layer 2 Ethernet packets.

This document specifies a new BGP-FS component type to support AS-level filtering. The match field is the origin AS number of the destination IP address that is encoded in the Flowspec NLRI. This function is applied in a single administrative domain.

2. Definitions and Acronyms

*FS: Flow Specification

*Destination-IP-Origin-AS: The origin AS number of the destination IP address

3. The Flow Specification Encoding for Destination-IP-Origin-AS Filter

This document proposes a new flow specification component type that is encoded in the BGP Flowspec NLRI. The following new component type is defined.

*Destination-IP-Origin-AS

Type TBD1 - Destination-IP-Origin-AS

Encoding: <type (1 octet), [op, value]+>

Contains a set of {operator, value} pairs that are used to match the Destination-IP-Origin-AS (i.e. the origin AS number of the destination IP address).

The operator byte is encoded as:

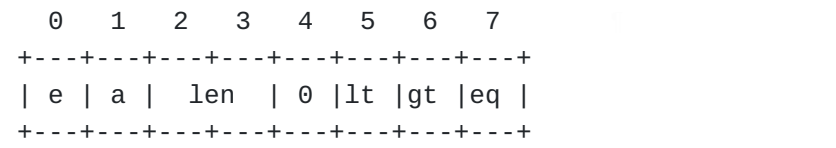

Figure 1: Numeric Operator (numeric_op)

Where:

e - end-of-list bit. Set in the last {op, value} pair in the list.

a - AND bit. If unset, the previous term is logically ORed with the current one. If set, the operation is a logical AND. It MUST be unset in the Destination-IP-Origin-AS filter.

len - The length of the value field for this operator given as (1 << len). This encodes 1 (len=00), 2 (len=01), 4 (len=10), and 8 (len=11) octets.

lt - less than comparison between data and value.

gt - greater than comparison between data and value.

eq - equality between data and value.

The bits lt, gt, and eq can be combined to produce match the Destination-IP-Origin-AS filter or a range of Destination-IP-Origin-AS filter(e.g. less than AS1 and greater than AS2).

The value field is encoded as:

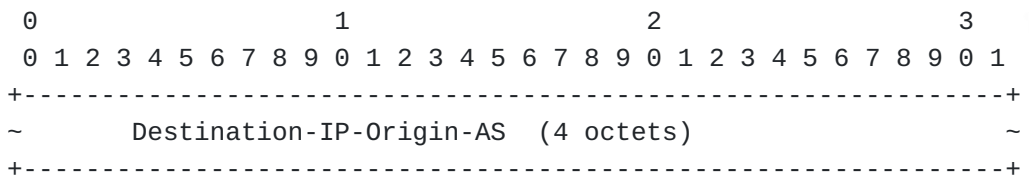

Figure 2: Destination-IP-Origin-AS

Per section 10 of [RFC8955] , If a receiving BGP speaker cannot support this new Flow Specification component type, it MUST discard the NLRI value field that contains such unknown components. Since the NLRI field encoding (Section 4 of [RFC8955]) is defined in the form of a 2-tuple <length, NLRI value>, message decoding can skip over the unknown NLRI value and continue with subsequent remaining NLRI.

4. Use Cases

This section describes how to use this function in a simple scenario. Considering the topology shown in Figure 3. In AS64597's R1, if the ISP AS64597 wants to redirect all packets originating from IP Prefix 61 to AS64598:

"first go to R3, then forward them to AS64598", the ISP AS64597 can use the traditional method or the method defining in this draft.

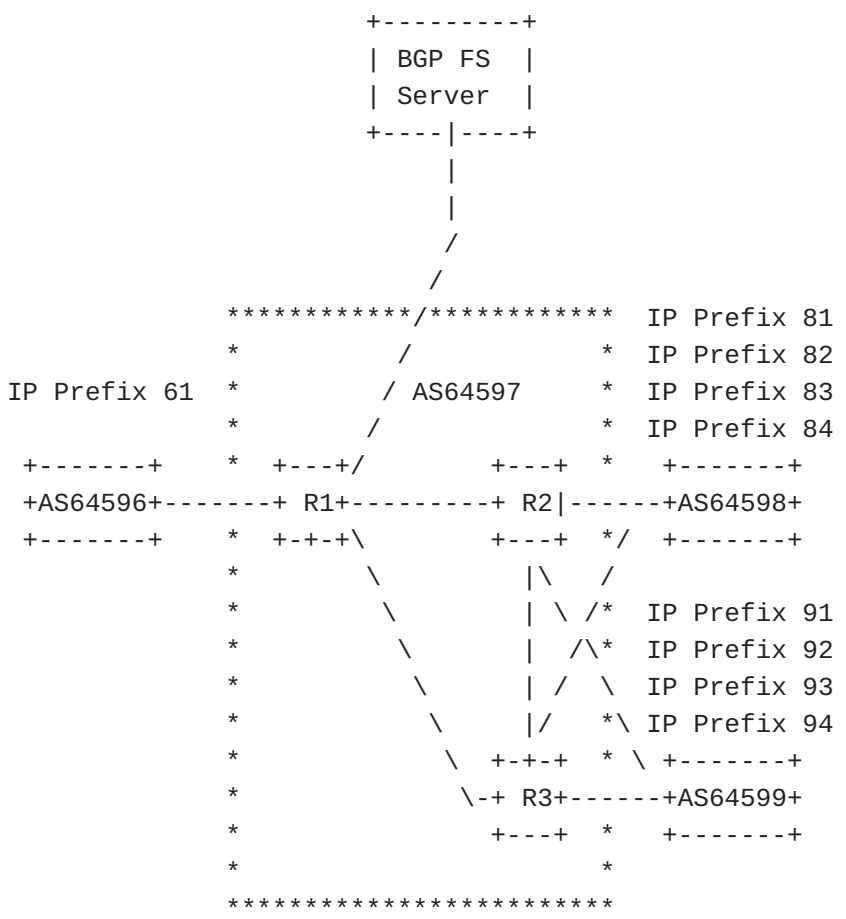

Figure 3: Redirect the traffic using Flowspec

Using the traditional method, the ISP AS64597 needs to setup multiple "Destination Prefix + Source Prefix" rules in Router R1 as following:

Destination Prefix	Source Prefix	Redirect to IP Nexthop
IP Prefix 81	IP Prefix 61	R3
IP Prefix 82	IP Prefix 61	R3
IP Prefix 83	IP Prefix 61	R3
IP Prefix 84	IP Prefix 61	R3
More ...		

Figure 4: Using the traditional method to redirect the traffic

Using the method defining in this draft, the ISP AS64597 needs to setup only one "Destination Origin AS + Source Prefix" rule in Router R1 as following:

Destination IP Origin AS	Source Prefix	Redirect to IP Nexthop
64598	IP Prefix 61	R3

Figure 5: Using the AS-level filtering method to redirect the traffic

Obviously, the new method defining in this draft saves a lot of entry spaces on the control plane and forwarding plane, and it would greatly simplify the operation of the control plane, and the more destination prefixes an AS has, the more obvious the benefit.

5. Security Considerations

No new security issues are introduced to the BGP protocol by this specification.

6. IANA

IANA is requested to a new entry in "Flow Spec component types registry" with the following values:

Type	RFC or Draft	Description
TBD1	This Draft	Destination-IP-Origin-AS

7. Contributors

TBD

8. Acknowledgments

The authors would like to acknowledge the review and inputs from Gang Yan, Robert Raszuk, Jeffray Haas, Linda Dunbar, Zhenbin Li, Rainbow Wu, Jie Dong and Ziqing Cao.

9. References

[I-D.ietf-idr-flowspec-l2vpn] Weiguo, H., Eastlake, D. E., Litkowski, S., and S. Zhuang, "BGP Dissemination of L2

Flow Specification Rules", Work in Progress, Internet-Draft, draft-ietf-idr-flowspec-l2vpn-20, 9 October 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-idr-flowspec-l2vpn-20>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC8955] Loibl, C., Hares, S., Raszuk, R., McPherson, D., and M. Bacher, "Dissemination of Flow Specification Rules", RFC 8955, DOI 10.17487/RFC8955, December 2020, <https://www.rfc-editor.org/info/rfc8955>.

[RFC8956] Loibl, C., Ed., Raszuk, R., Ed., and S. Hares, Ed., "Dissemination of Flow Specification Rules for IPv6", RFC 8956, DOI 10.17487/RFC8956, December 2020, <https://www.rfc-editor.org/info/rfc8956>.

Authors' Addresses

Haibo Wang
Huawei
156 Beiqing Road
Beijing
100095
P.R. China

Email: rainsword.wang@huawei.com

Aijun Wang
China Telecom
Beiqijia Town, Changping District
Beijing
102209
P.R. China

Email: wangaj3@chinatelecom.cn

Shunwan Zhuang
Huawei
156 Beiqing Road
Beijing
100095

P.R. China

Email: zhuangshunwan@huawei.com