IDR Working Group
Internet-Draft
Intended status: Informational
Expires: 26 June 2026

X. Ding
Z. Tan
L. Wang
Huawei Technologies

23 December 2025

Route Target Constraint for BGP Flow Spec(BGP Flow) and BGP Segment Routing Policies(BGP SR-Policy) draft-ding-idr-rtc-for-bgp-flow-sr-01

Abstract

This document specifies an extension to the application scenarios of Route Target Constraints (RTC). By using the Global Administrator field of the IPv4 Address Specific Extended Community to identify a network node and exchanging BGP Route-Target routes, a BGP speaker can generate an egress policy for filtering routing updates associated with specific network nodes,which could implement precise control and distribution of services such as BGP Flow Specification and BGP Segment Routing Policies.

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 RFC 2119 [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 26 June 2026.

Table of Contents

1. Introduction

BGP [RFC4271] has been used to distribute different types of routing and policy information. In some scenarios, the distributed routing information is specific for certain services, such as BGP/MPLS IP VPNs.

Route Target Constraints (RTC) [RFC4684], extends Outbound Route Filtering (ORF), describes how route targets are exchanged through the BGP RTC address family on a BGP/MPLS IP VPN network to generate egress policies. This feature enables the BGP/MPLS IP VPN network to control the advertisement of VPN routing information in a more refined manner.

This document introduces an extension to the application scenarios of Route Target Constraints (RTC) [RFC4684] to control the distribution of routing information to one or a group of network nodes, which could implement precise control of services such as BGP Flow Spec [RFC8955] and BGP Segment Routing Policies [I-D.ietf-idr-segment-routing-te-policy].

1.1. Terminology

This document introduces the following terms:

RTC Route Target Constraints [RFC 4684]

ORF Outbound Route Filtering

Flowspec BGP Flow Specification

SR-Policy BGP Segment Routing Policy

NLRI Network Layer Reachability Information

2. Route Target Membership NLRI Advertisements

The encapsulation of Route Target membership NLRI is defined in Route Target Constraints (RTC) [RFC4684], the NLRI is advertised in BGP UPDATE messages using the MP_REACH_NLRI and MP_UNREACH_NLRI attributes. The (AFI, SAFI) value pair used to identify this NLRI is (AFI=1, SAFI=132).

The route-target field in the NLRI indicates a network node and is encoded as a IPv4 Address Specific Extended Community [RFC4360], as shown blow:

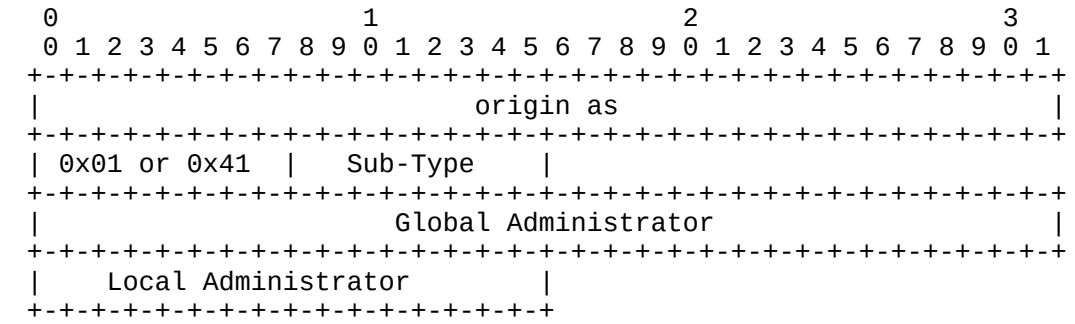

Figure 1: Route Target membership NLRI Format

While encoding these fields:

* Global Administrator: 4 octets, indicates the router identifier of the node. If the Global Administrator is set to 0.0.0.0, it means that the peer node accepts all policy rules from the RR.

* Local Administrator: 2 octets, reserved for future use, MUST be set to 0 upon the sender and MUST be ignored upon the receiver.

3. Use case

This section describes a few use-case scenarios.

3.1. BGP Flow Spec ORF

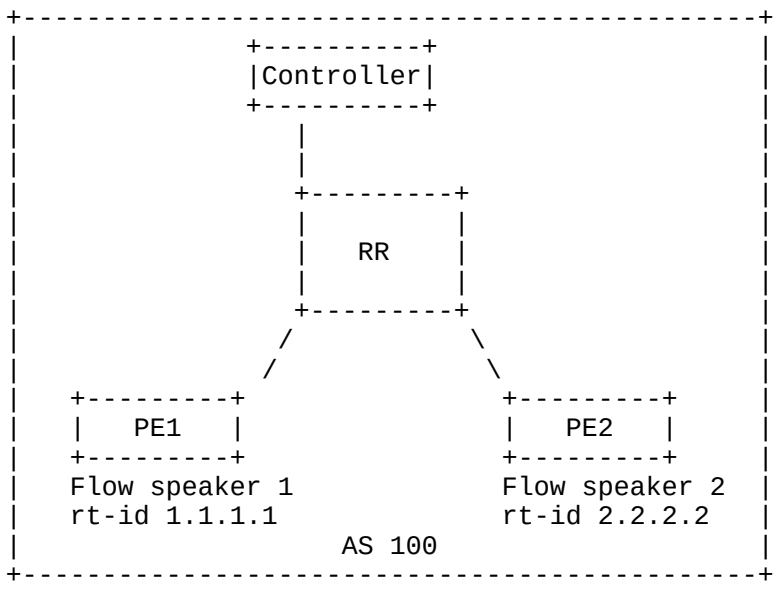

Figure 2: BGP Flow Spec ORF

In the topology above, the Controller, PE1, and PE2 establish IBGP peer relationships with the RR respectively. PE1 and PE2 are clients of the RR. The Controller distributes Flowspec rules through the RR, and the RR reflects the Flowspec rules to PE1 and PE2.

PE1 sends route target membership NLRI{100, 1.1.1.1:0} to the RR, and PE2 sends route target membership NLRI{100, 2.2.2.2:0} to the RR. After receiveing the UPDATE messages with Route Target Membership NLRI, the RR will trigger the RIB-OUTS of the Flowspec route to match the egress policies and update the route to PEs.

If hierarchical RRs are deployed, the RRs need to advertise all received route target membership NLRI routes to the upper-layer RRs.

3.2. BGP Segment Routing Policies ORF

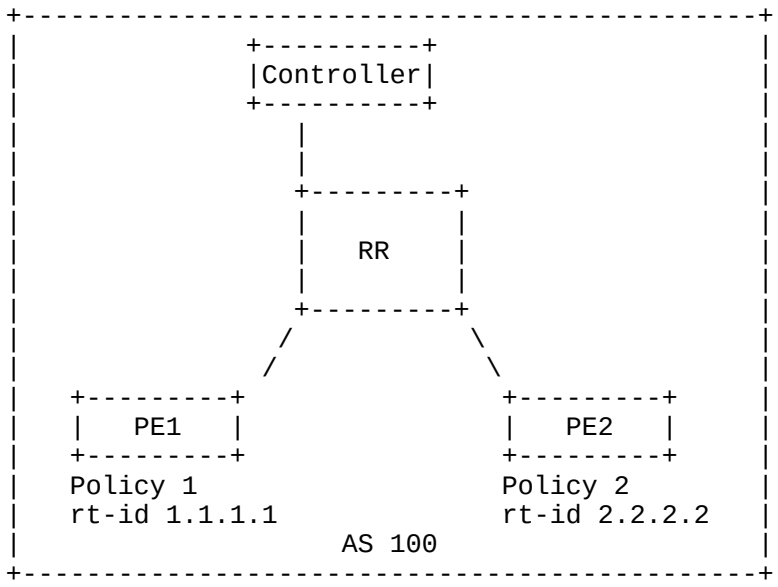

Figure 3: BGP Segment Routing Policies ORF

It is described in BGP Segment Routing Policies [I-D.ietf-idr-segment-routing-te-policy] that one or more route targets SHOULD be attached to the advertisement, where each route target identifies one or more intended headends for the advertised SR Policy update. In the topology above, when the controller needs to deliver SR policies to PE1 and PE2, it will advertises SR policies with route target extended communities, SR Policy1 with {1.1.1.1:0} and SR Policy2 with {2.2.2.2:0}, to RR. The RR will reflect SR Policies to both PE1 and PE2. PEs need to do an ingress filtering, by matching route target extended community with its own router-id. In this case, PE1 will keep SR Policy1 and drop SR Policy2, as well as PE2 will keep SR Policy2 and drop SR Policy1. During this process, even though SR policies are correctly provisioned, the RR advertises all routes to all peers, which may cause network congestion.

The ORF operations described in this document work as an egress filter on RR. PE1 sends route target membership NLRI{100, 1.1.1.1:0} to the RR, and PE2 sends route target membership NLRI{100, 2.2.2.2:0} to the RR. After receiving the Route Target Membership NLRI from the

PE, the RR generates a PE-specific egress filter. Before advertising routes to PEs, the RR matches routes with egress policies, and will only deliver SR policy1 to PE1 and SR policy1 to PE2 respectively. In this way, services could be correctly deployed and network bandwidth could be saved.

4. IANA Considerations

TBD

5. Security Considerations

TBD

6. References

6.1. Normative References

[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>.

[RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, DOI 10.17487/RFC4360, February 2006, <https://www.rfc-editor.org/info/rfc4360>.

[RFC4684] Marques, P., Bonica, R., Fang, L., Martini, L., Raszuk, R., Patel, K., and J. Guichard, "Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)", RFC 4684, DOI 10.17487/RFC4684, November 2006, <https://www.rfc-editor.org/info/rfc4684>.

6.2. References

[I-D.ietf-idr-segment-routing-te-policy] Previdi, S., Filsfils, C., Talaulikar, K., Mattes, P., and D. Jain, "Advertising Segment Routing Policies in BGP", Work in Progress, Internet-Draft, draft-ietf-idr-segment-routing-te-policy-26, 23 October 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-idr-segment-routing-te-policy-26>.

[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>.

Authors' Addresses

Xiangfeng Ding
Huawei Technologies
No. 156 Beiqing Road
Beijing
100095
P.R. China
Email: dingxiangfeng@huawei.com

Zhen Tan
Huawei Technologies
No. 156 Beiqing Road
Beijing
100095
P.R. China
Email: tanzhen6@huawei.com

Lili Wang
Huawei Technologies
No. 156 Beiqing Road
Beijing
100095
P.R. China
Email: lily.wong@huawei.com