

Global Routing Operations
Internet-Draft
Updates: [7854](#) (if approved)
Intended status: Standards Track
Expires: June 22, 2019

T. Evens
S. Bayraktar
Cisco Systems
P. Lucente
NTT Communications
P. Mi
Tencent
S. Zhuang
Huawei
December 19, 2018

Support for Adj-RIB-Out in BGP Monitoring Protocol (BMP)
draft-ietf-grow-bmp-adj-rib-out-03

Abstract

The BGP Monitoring Protocol (BMP) defines access to only the Adj-RIB-In Routing Information Bases (RIBs). This document updates the BGP Monitoring Protocol (BMP) [RFC 7854](#) by adding access to the Adj-RIB-Out RIBs. It adds a new flag to the peer header to distinguish Adj-RIB-In and Adj-RIB-Out.

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 June 22, 2019.

Copyright Notice

Copyright (c) 2018 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 (<https://trustee.ietf.org/license-info>) in effect on the date of

Internet-Draft

BMP Adj-RIB-Out

December 2018

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology	3
3.	Definitions	3
4.	Per-Peer Header	4
5.	Adj-RIB-Out	4
5.1.	Post-Policy	4
5.2.	Pre-Policy	4
6.	BMP Messages	5
6.1.	Route Monitoring and Route Mirroring	5
6.2.	Statistics Report	5
6.3.	Peer Down and Up Notifications	6
6.3.1.	Peer Up Information	6
7.	Other Considerations	6
7.1.	Peer and Update Groups	6
8.	Security Considerations	7
9.	IANA Considerations	7
9.1.	BMP Peer Flags	7
9.2.	BMP Statistics Types	7
9.3.	Peer UP Information TLV	8
10.	References	8
10.1.	Normative References	8
10.2.	URIs	8
	Acknowledgements	9
	Contributors	9
	Authors' Addresses	9

[1.](#) Introduction

BGP Monitoring Protocol (BMP) defines monitoring of the received (e.g. Adj-RIB-In) Routing Information Bases (RIBs) per peer. The Adj-RIB-In pre-policy conveys to a BMP receiver all RIB data before any policy has been applied. The Adj-RIB-In post-policy conveys to a BMP receiver all RIB data after policy filters and/or modifications have been applied. An example of pre-policy verses post-policy is

when an inbound policy applies attribute modification or filters. Pre-policy would contain information prior to the inbound policy changes or filters of data. Post policy would convey the changed data or would not contain the filtered data.

Monitoring the received updates that the router received before any policy has been applied is the primary level of monitoring for most use-cases. Inbound policy validation and auditing is the primary use-case for enabling post-policy monitoring.

In order for a BMP receiver to receive any BGP data, the BMP sender (e.g. router) needs to have an established BGP peering session and actively be receiving updates for an Adj-RIB-In.

Being able to only monitor the Adj-RIB-In puts a restriction on what data is available to BMP receivers via BMP senders (e.g. routers). This is an issue when the receiving end of the BGP peer is not enabled for BMP or when it is not accessible for administrative reasons. For example, a service provider advertises prefixes to a customer, but the service provider cannot see what it advertises via BMP. Asking the customer to enable BMP and monitoring of the Adj-RIB-In is not feasible.

This document updates BGP Monitoring Protocol (BMP) [RFC 7854](#) [[RFC7854](#)] peer header by adding a new flag to distinguish Adj-RIB-In verses Adj-RIB-Out.

Adding Adj-RIB-Out enables the ability for a BMP sender to send to a BMP receiver what it advertises to BGP peers, which can be used for outbound policy validation and to monitor RIBs that were advertised.

[2.](#) Terminology

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](#)].

[3.](#) Definitions

- o Adj-RIB-Out: As defined in [[RFC4271](#)], "The Adj-RIBs-Out contains the routes for advertisement to specific peers by means of the

local speaker's UPDATE messages."

- o Pre-Policy Adj-RIB-Out: The result before applying the outbound policy to an Adj-RIB-Out. This normally would match what is in the local RIB.
- o Post-Policy Adj-RIB-Out: The result of applying outbound policy to an Adj-RIB-Out. This MUST be what is actually sent to the peer.

[4.](#) Per-Peer Header

The per-peer header has the same structure and flags as defined in [section 4.2 \[RFC7854\]](#) with the following 0 flag addition:

```
    0 1 2 3 4 5 6 7
    +---+---+---+---+
    |V|L|A|0| Resv |
    +---+---+---+---+
```

- o The 0 flag indicates Adj-RIB-In if set to 0 and Adj-RIB-Out if set to 1.

The existing flags are defined in [section 4.2 \[RFC7854\]](#) and the remaining bits are reserved for future use. They SHOULD be transmitted as 0 and their values MUST be ignored on receipt. The following fields in Per-Peer Header are redefined:

- o Peer Address: The remote IP address associated with the TCP session over which the encapsulated PDU was sent.
- o Peer AS: The Autonomous System number of the peer from which the encapsulated PDU was sent.
- o Peer BGP ID: The BGP Identifier of the peer from which the encapsulated PDU was sent.

[5.](#) Adj-RIB-Out

[5.1.](#) Post-Policy

The primary use-case in monitoring Adj-RIB-Out is to monitor the updates transmitted to the BGP peer after outbound policy has been applied. These updates reflect the result after modifications and filters have been applied (e.g. Adj-RIB-Out Post-Policy). Some attributes are set when the BGP message is transmitted, such as next-hop. Adj-RIB-Out Post-Policy MUST convey what is actually transmitted to the peer, next-hop and any attribute set during transmission should also be set and transmitted to the BMP receiver.

The L flag MUST be set to 1 to indicate post-policy.

[5.2.](#) Pre-Policy

As with Adj-RIB-In policy validation, there are use-cases that pre-policy Adj-RIB-Out is used to validate and audit outbound policies. For example, a comparison between pre-policy and post-policy can be used to validate the outbound policy.

Depending on BGP peering session type (IBGP, IBGP route reflector client, EBGP, BGP confederations, Route Server Client) the candidate routes that make up the Pre-Policy Adj-RIB-Out do not contain all local-rib routes. Pre-Policy Adj-RIB-Out conveys only routes that are available based on the peering type. Post-Policy represents the filtered/changed routes from the available routes.

Some attributes are set only during transmission of the BGP message, e.g. Post-Policy. It is common that next-hop may be null, loopback, or similar during this phase. All mandatory attributes, such as next-hop, MUST be either ZERO or have an empty length if they are unknown at the Pre-Policy phase. The BMP receiver will treat zero or empty mandatory attributes as self originated.

The L flag MUST be set to 0 to indicate pre-policy.

[6.](#) BMP Messages

Many BMP messages have a per-peer header but some are not applicable to Adj-RIB-In or Adj-RIB-Out monitoring. Unless otherwise defined, the O flag should be set to 0 in the per-peer header in BMP messages.

[6.1.](#) Route Monitoring and Route Mirroring

The 0 flag MUST be set accordingly to indicate if the route monitor or route mirroring message conveys Adj-RIB-In or Adj-RIB-Out.

[6.2.](#) Statistics Report

Statistics report message has Stat Type field to indicate the statistic carried in the Stat Data field. Statistics report messages are not specific to Adj-RIB-In or Adj-RIB-Out and MUST have the 0 flag set to zero. The 0 flag SHOULD be ignored by the BMP receiver.

The following new statistic types are added:

- o Stat Type = 14: (64-bit Gauge) Number of routes in Adj-RIBs-Out Pre-Policy.
- o Stat Type = 15: (64-bit Gauge) Number of routes in Adj-RIBs-Out Post-Policy.
- o Stat Type = 16: Number of routes in per-AFI/SAFI Adj-RIB-Out Pre-Policy. The value is structured as: 2-byte Address Family Identifier (AFI), 1-byte Subsequent Address Family Identifier (SAFI), followed by a 64-bit Gauge.

- o Stat Type = 17: Number of routes in per-AFI/SAFI Adj-RIB-Out Post-Policy. The value is structured as: 2-byte Address Family Identifier (AFI), 1-byte Subsequent Address Family Identifier (SAFI), followed by a 64-bit Gauge.

[6.3.](#) Peer Down and Up Notifications

PEER UP and DOWN notifications convey BGP peering session state to BMP receivers. The state is independent of whether or not route monitoring or route mirroring messages will be sent for Adj-RIB-In, Adj-RIB-Out, or both. BMP receiver implementations SHOULD ignore the 0 flag in PEER UP and DOWN notifications. BMP receiver implementations MUST use the per-peer header 0 flag in route monitoring and mirroring messages in order to identify if the message is for Adj-RIB-In or Adj-RIB-Out.

[6.3.1.](#) Peer Up Information

The following peer UP information TLV types are added:

- o Type = 4: Admin Label. The Information field contains a free-form UTF-8 string whose length is given by the Information Length field. The value is administratively assigned. There is no requirement to terminate the string with null or any other character.

Multiple admin labels can be included in the Peer UP. When multiple admin labels are included the BMP receiver MUST preserve the order.

The TLV is optional.

[7.](#) Other Considerations

[7.1.](#) Peer and Update Groups

Peer and update groups are used to group updates shared by many peers. This is a level of efficiency in the implementation, not a true representation of what is conveyed to a peer in either Pre-Policy or Post-Policy.

One of the use-cases to monitor Adj-RIB-Out Post-Policy is to validate and continually ensure the egress updates match what is expected. For example, wholesale peers should never have routes with community X:Y sent to them. In this use-case, there maybe hundreds of wholesale peers but a single peer could have represented the group.

A single peer could be used to represent a group. From a BMP perspective, this should be simple to include a group name in the PEER UP, but it is more complex than that. BGP implementations have evolved to provide comprehensive and structured policy grouping, such as session, afi/safi, and template based group policy inheritances.

This level of structure and inheritance of polices does not provide a simple peer group name or ID, such as wholesale peer.

Instead of requiring a group name to be used, a new administrative label informational TLV ([Section 6.3.1](#)) is added to the Peer UP message. These labels have administrative scope relevance. For example, labels "type=wholesale" and "region=west" could be used to monitor expected policies.

Configuration and assignment of labels to peers is BGP implementation specific.

[8.](#) Security Considerations

It is not believed that this document adds any additional security considerations.

[9.](#) IANA Considerations

This document requests that IANA assign the following new parameters to the BMP parameters name space [[1](#)].

[9.1.](#) BMP Peer Flags

This document defines the following new per-peer header flags ([Section 4](#)):

- o Flag 3 as 0 flag: The 0 flag indicates Adj-RIB-In if set to 0 and Adj-RIB-Out if set to 1.

[9.2.](#) BMP Statistics Types

This document defines four new statistic types for statistics reporting ([Section 6.2](#)):

- o Stat Type = 14: (64-bit Gauge) Number of routes in Adj-RIBs-Out Pre-Policy.
- o Stat Type = 15: (64-bit Gauge) Number of routes in Adj-RIBs-Out Post-Policy.

- o Stat Type = 16: Number of routes in per-AFI/SAFI Adj-RIB-Out Pre-

Policy. The value is structured as: 2-byte Address Family Identifier (AFI), 1-byte Subsequent Address Family Identifier (SAFI), followed by a 64-bit Gauge.

- o Stat Type = 17: Number of routes in per-AFI/SAFI Adj-RIB-Out Post-Policy. The value is structured as: 2-byte Address Family Identifier (AFI), 1-byte Subsequent Address Family Identifier (SAFI), followed by a 64-bit Gauge.

9.3. Peer UP Information TLV

This document defines the following new BMP PEER UP informational message TLV types ([Section 6.3.1](#)):

- o Type = 4: Admin Label. The Information field contains a free-form UTF-8 string whose length is given by the Information Length field. The value is administratively given by the Information Length field. The value is administratively assigned. There is no requirement to terminate the string with null or any other character.

10. References

10.1. 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>>.
- [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>>.
- [RFC7854] Scudder, J., Ed., Fernando, R., and S. Stuart, "BGP Monitoring Protocol (BMP)", [RFC 7854](#), DOI 10.17487/RFC7854, June 2016, <<https://www.rfc-editor.org/info/rfc7854>>.

10.2. URIs

- [1] <https://www.iana.org/assignments/bmp-parameters/bmp-parameters.xhtml>

Acknowledgements

The authors would like to thank John Scudder for his valuable input.

Contributors

Manish Bhardwaj
Cisco Systems
3700 Cisco Way
San Jose, CA 95134
USA

Email: manbhard@cisco.com

Xianyuzheng
Tencent
Tencent Building, Kejizhongyi Avenue,
Hi-techPark, Nanshan District, Shenzhen 518057, P.R.China

Weiguo
Tencent
Tencent Building, Kejizhongyi Avenue,
Hi-techPark, Nanshan District, Shenzhen 518057, P.R.China

Shugang cheng
H3C

Authors' Addresses

Tim Evens
Cisco Systems
2901 Third Avenue, Suite 600
Seattle, WA 98121
USA

Email: tievens@cisco.com

Internet-Draft

BMP Adj-RIB-Out

December 2018

Serpil Bayraktar
Cisco Systems
3700 Cisco Way
San Jose, CA 95134
USA

Email: serpil@cisco.com

Paolo Lucente
NTT Communications
Siriusdreef 70-72
Hoofddorp, WT 2132
NL

Email: paolo@ntt.net

Penghui Mi
Tencent
Tengyun Building, Tower A ,No. 397 Tianlin Road
Shanghai 200233
China

Email: kevinmi@tencent.com

Shunwan Zhuang
Huawei
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China

Email: zhuangshunwan@huawei.com

