Internet Engineering Task Force (IETF)
Request for Comments: 8671
Updates: 7854
Category: Standards Track
ISSN: 2070-1721

T. Evens
S. Bayraktar
Cisco Systems
P. Lucente
NTT Communications
P. Mi
Tencent
S. Zhuang
Huawei

November 2019

Support for Adj-RIB-Out in the BGP Monitoring Protocol (BMP)

Abstract

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

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8671.

Table of Contents

1. Introduction

The BGP Monitoring Protocol (BMP) defines monitoring of the received (e.g., Adj-RIB-In) Routing Information Bases (RIBs) per peer. The pre-policy Adj-RIB-In conveys to a BMP receiver all RIB data before any policy has been applied. The post-policy Adj-RIB-In conveys to a BMP receiver all RIB data after policy filters and/or modifications have been applied. An example of pre-policy versus 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 are the primary use cases 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 are not feasible.

BMP [RFC7854] only defines Adj-RIB-In being sent to BMP receivers. This document updates the per-peer header defined in Section 4.2 of [RFC7854] by adding a new flag to distinguish between Adj-RIB-In and

Adj-RIB-Out. BMP senders use the new flag to send either Adj-RIB-In or Adj-RIB-Out.

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

2. Terminology

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. Definitions

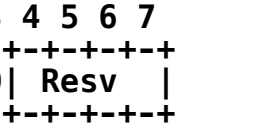
Adj-RIB-Out
: As defined in [RFC4271], "The Adj-RIBs-Out contains the routes for advertisement to specific peers by means of the local speaker's UPDATE messages."

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.

Post-policy Adj-RIB-Out
: The result of applying outbound policy to an Adj-RIB-Out. This MUST convey to the BMP receiver what is actually transmitted to the peer.

4. Per-Peer Header

The per-peer header has the same structure and flags as defined in Section 4.2 of [RFC7854] with the addition of the O flag as shown here:



* The O 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 of [RFC7854], and the remaining bits are reserved for future use. They MUST be transmitted as 0, and their values MUST be ignored on receipt.

When the O flag is set to 1, the following fields in the per-peer header are redefined:

* Peer Address: The remote IP address associated with the TCP session over which the encapsulated Protocol Data Unit (PDU) is sent.

* Peer AS: The Autonomous System number of the peer to which the encapsulated PDU is sent.

* Peer BGP ID: The BGP Identifier of the peer to which the encapsulated PDU is sent.

* Timestamp: The time when the encapsulated routes were advertised (one may also think of this as the time when they were installed in the Adj-RIB-Out), expressed in seconds and microseconds since midnight (zero hour), January 1, 1970 (UTC). If zero, the time is unavailable. Precision of the timestamp is implementation-dependent.

5. Adj-RIB-Out

5.1. Post-policy

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

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

5.2. Pre-policy

Similar to Adj-RIB-In policy validation, pre-policy Adj-RIB-Out can be 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 the BGP peering session type -- Internal BGP (IBGP), IBGP route reflector client, External BGP (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, i.e., post-policy. It is common that the next hop may be null, loopback, or similar during the pre-policy 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 completion. 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, such as Peer Up and Down Notifications. 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 O 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

The Statistics Report message has a 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 O flag set to zero. The O flag SHOULD be ignored by the BMP receiver.

This document defines the following new statistics types:

* Stat Type = 14: Number of routes in pre-policy Adj-RIB-Out. This statistics type is 64-bit Gauge.

* Stat Type = 15: Number of routes in post-policy Adj-RIB-Out. This statistics type is 64-bit Gauge.

* Stat Type = 16: Number of routes in per-AFI/SAFI pre-policy Adj-RIB-Out. The value is structured as: 2-byte Address Family Identifier (AFI), 1-byte Subsequent Address Family Identifier (SAFI), followed by a 64-bit Gauge.

* Stat Type = 17: Number of routes in per-AFI/SAFI post-policy Adj-RIB-Out. 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 Up and Down 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 O flag in Peer Up and Down Notifications.

6.3.1. Peer Up Information

This document defines the following Peer Up Information TLV type:

* Type = 4: Admin Label. The Information field contains a free-form UTF-8 string whose byte 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 Notification. When multiple Admin Labels are included, the BMP receiver MUST preserve their order.

The Admin Label 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 implementations, 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 post-policy Adj-RIB-Out 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 may be hundreds of wholesale peers, but a single peer could have represented the group.

From a BMP perspective, it 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.

This document defines a new Admin Label type for Peer Up Information TLVs (Section 6.3.1) that can be used instead of requiring a group name. 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 are BGP implementation-specific.

7.2. Changes to Existing BMP Session

In case of any change that results in the alteration of behavior of an existing BMP session (i.e., changes to filtering and table names), the session MUST be bounced with a Peer Down/Peer Up sequence.

8. Security Considerations

The considerations in Section 11 of [RFC7854] apply to this document. Implementations of this protocol SHOULD require establishing sessions with authorized and trusted monitoring devices. It is also believed that this document does not add any additional security considerations.

9. IANA Considerations

IANA has assigned the following new parameters to the "BGP Monitoring Protocol (BMP) Parameters" registry (https://www.iana.org/assignments/bmp-parameters/).

9.1. Addition to BMP Peer Flags Registry

IANA has made the following assignment for the per-peer header flag defined in Section 4 of this document:

Flag	Description	Reference
3	O flag	RFC 8671

Table 1: Addition to the "BMP Peer Flags" Registry

9.2. Additions to BMP Statistics Types Registry

IANA has made the following assignment for the four statistics types defined in Section 6.2 of this document:

Stat Type	Description	Reference
14	Number of routes in pre-policy Adj-RIB-Out	RFC 8671
15	Number of routes in post-policy Adj-RIB-Out	RFC 8671
16	Number of routes in per-AFI/SAFI pre-policy Adj-RIB-Out	RFC 8671
17	Number of routes in per-AFI/SAFI post-policy Adj-RIB-Out	RFC 8671

Table 2: Additions to the "BMP Statistics Types" Registry

9.3. Addition to BMP Initiation Message TLVs Registry

IANA has made the following assignment per Section 6.3.1 of this document:

Type	Description	Reference
4	Admin Label	RFC 8671

Table 3: Addition to the "BMP Initiation Message TLVs" Registry

10. 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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Acknowledgements

The authors would like to thank John Scudder and Mukul Srivastava for their valuable input.

Contributors

The following individuals contributed to this document:

* Manish Bhardwaj, Cisco Systems

* Xianyu Zheng, Tencent

* Wei Guo, Tencent

* Shugang Cheng, H3C

Authors' Addresses

Tim Evens
Cisco Systems
2901 Third Avenue, Suite 600
Seattle, WA 98121
United States of America

Email: tievens@cisco.com

Serpil Bayraktar
Cisco Systems
3700 Cisco Way
San Jose, CA 95134
United States of America

Email: serpil@cisco.com

Paolo Lucente

NTT Communications
Siriusdreef 70-72
2132 Hoofddorp
Netherlands

Email: paolo@ntt.net

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

Email: Penghui.Mi@gmail.com

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

Email: zhuangshunwan@huawei.com