Global Routing Operations
Internet-Draft
Updates: 7854 (if approved)
Intended status: Standards Track
Expires: 9 January 2025

P. Lucente
C. Cardona
NTT

8 July 2024

Logging of Routing events Events in BGP Monitoring Protocol (BMP)

draft-ietf-grow-bmp-rel-02

Abstract

The BGP Monitoring Protocol (BMP) does provision for BGP session event logging (Peer Up, Peer Down), state synchronization (Route Monitoring), debugging (Route Mirroring) and Statistics messages, among the others. This document defines a new Route Event Logging (REL) message type for BMP with the aim of covering use- cases with affinity to alerting, reporting, and on-change analysis.

Commenté [MB1]: Not sure to parse this.

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 9 January 2025.

Copyright Notice

Table of Contents

1. Introduction

As NLRIs are advertised and distributed, policies are applied and, as a result, actions are performed on them. Currently, in order to infer the outcome of an evaluation process, a comparative analysis needs to be performed between Route Monitoring data for two distinct observation points of interest, for example pre-policy and Post-Policy Adj-Rib-In ~~pre-policy and post-policy~~. It would be instead more useful if a monitored router could export event-driven data with the relevant information.

The envisioned use~~-~~ cases are ~~the most~~ diverse and range from logging route filtering to reporting the outcome of validation processes taking place on ~~the~~ a monitored router, to isolating certain subsets of data to be validated offline, to report malformed BGP packets, to broader closed-loop operations.

Since no other existing BGP Monitoring Protocol (BMP) [RFC7854] message type does fit the described purpose, this document defines a new Route Event Logging (REL) message type that is suitable to carry event-driven data and is extensible in nature. While the REL message format is similar to the Route Mirroring message type ~~defined in RFC 7854~~ (Section 5 of [RFC7854]) and to the Route Monitoring message type ~~as~~ defined in TLV ~~support~~ Support for BMP Route Monitoring and Peer Down Messages [I-D.ietf-grow-bmp-tlv], the semantics are different.

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 RFC 2119 [RFC2119] RFC 8174 [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document makes use of the terms defined in [RFC7854].

Commenté [MB2]: Please expand, mention BGP + Cite RFC 4271

Commenté [MB3]: Please be explicit as to which this refers to.

Commenté [MB4]: Which evaluation? Please be explicit

Commenté [MB5]: Be consistent with 7854 use

Commenté [BMI6]: Point to where this clarified in the document

3. Route Event Logging (REL) Mmessage

In bBasically, terms a REL message does carry Events. Each Event is logically composed by one Event Subject and one or more Event Attributes.

The structure of the Route Event Logging message is the same as the Route Monitoring message defined in "TLV support Support for BMP Route Monitoring and Peer Down Messages" [I-D.ietf-grow-bmp-tlv] where the Per-Peer Header is followed by a BGP Message TLV, one indexed Informational TLV, and further optional indexed Informational TLVs. An example of such structure is available in Section 4.2.1.1 of [I-D.ietf-grow-bmp-tlv].

One or more Event Subjects are packed as part of a BGP Update PDU. The BGP Update PDU (Section 4.3 of [RFC4271]) is encoded itself as part of a BGP Message TLV with code point TBD1 and index set to zero. Each Event Subject is represented by an NLRI carried in the PDU.

The BGP Message TLV may be precededpreceded and/or followed by indexed Informational TLVs that carry Event Attributes, where attributes are bound to subjects referring to their positional index within the PDU or via a Group TLV as described in Section 4.2.1 of [I-D.ietf-grow-bmp-tlv]

a mis en forme : Surlignage

Speaking comparatively to other existing message types, REL does not require an initial flooding of information as per the state synchronization nature of Route Monitoring. Likewise, it and does not aim to provide a non-state-compressed full-fidelity view of all messages received as per the debugging nature of Route Mirroring.

In the context of BMP REL message, and hence in the reminder of this document, the term Event Subject and NLRI will be used interchangeably. Also, the term Event Attribute and Informational TLV will be used interchangeably.

The following sections will describe each component of the REL message in more detail.

3.1. Per-Peer Header

The REL message does starts with a BMP per-peer header as defined in RFC 7854 [RFC7854], subsequently extended by RFC 8671 [RFC8671], and RFC 9069 [RFC9069] allowing, among the other things, to timestamp an Event and set its observation point among those defined in BMP.

Commenté [MB7]: Add the section where this is defined

Because the main purpose of the REL message is to log events at the time of applying an action, the Peer Flags field - even if applied to Adj-Rib-In or Adj-Rib-Out does not have the concept of pre- and post-policy. The flags are hence defined as follows:

a mis en forme : Surlignage

```
+-+-+-+-+-+-+-+-+
|V|A| Reserved   Unassigned   |
+-+-+-+-+-+-+-+-+
```

The V flag and A flag do carry the same meaning as originally defined by in Section 4.2 of RFC 7854 [RFC7854]. The remaining bits are Unassigned and reserved for future use. They MUST be transmitted as 0 and their values MUST be ignored on receipt.

3.2. BGP Update PDU

The PDU enclosed as part of a BGP Message TLV can be either a verbatim copy or artificial, either packed from scratch or repacked starting from an existing BGP Update PDU to only contain the relevant NLRIs affected by an Event (one or multiple). The Event is going to be further described by means of Event Attributes by indexed Informational TLVs.

The choice of describing one or multiple Event Subjects via a BGP Update PDU is because, on one hand, this does allow to not have to invent new encodings for NLRIs, while on the other, to support all types and encodings already supported by BGP. The advantage being that only minimal new code, on both the exporting and the receiving sides, will have to be produced.

3.3. Informational TLVs

BMP Informational TLVs ~~in BMP~~ are formalized by the intersection of RFC 7854 [RFC7854], TLV support for BMP Route Monitoring and Peer Down Messages [I-D.ietf-grow-bmp-tlv] and Support for Enterprise- specific TLVs in the BGP Monitoring Protocol [I-D.ietf-grow-bmp-tlv-ebit]. TLVs in a REL message are indexed.

Contrary to other BMP messages where all Informational TLVs are entirely optional, in order for a REL message to be meaningful, ~~it~~a REL message MUST contain at least one Event Reason TLV and MAY contain other ~~optional~~ attribute TLVs to further characterize the Event.

A new registry called "Route Event Logging TLVs" is defined and is seeded with the TLVs detailed in the following sections.

3.3.1. Event Reason TLV

TBD2 = Event Reason TLV (4 octets). Indicates the IANA-registered reason code describing the type of the event. The following reason codes are defined as part of the "Event Reason TLV" registry:

Value	Reason
0x0000	Unknown
0x0001	Log Action
0x0002	Policy Discard
0x0004	Validation Fail

Commenté [MB8]: RFC8176 says the following:

«Reserved: Not assigned and not available for assignment. Reserved values are held for special uses, such as to extend the namespace when it becomes exhausted. "Reserved" is also sometimes used to designate values that had been assigned but are no longer in use, keeping them set aside as long as other unassigned values are available. Note that this is distinctly different from "Unassigned". »

a mis en forme : Surlignage

a mis en forme : Surlignage

Commenté [BMI9]: Can be tagged as an implementation note

Commenté [MB10]: ??

Commenté [MB11]: Redundant with MAY

Commenté [MB12]: Move to IANA section

Commenté [BMI13]: Can the a log event in theory match several reasons?

0x0008	Malformed Packet
0x0010	Crossed Warning Bound
0x0020	Crossed Upper Bound

Table 1: Event Reason Codes

3.3.2. Policy Discard TLV

TBD3 = Policy Discard TLV. The value contains a UTF-8 string whose value can be organized freely by an implementation. For example, it may contain the routing policy name that caused the discard; or it may list a sequence of policies and policy nodes traversed; or, more simply, it could be a meaningful return code.

~~On the escort of~~Given Section 4 of [RFC9067] and YANG Model for Border Gateway Protocol (BGP-4) [I-D.ietf-idr-bgp-model] it is RECOMMENDED to organize the string as a comma-separated string with the policy definition name being followed by the statement name.

3.3.3. Malformed Packet TLV

TBD8 = Malformed Packet TLV. The length is to be set to 2 bytes and the value represents a code giving more information about the specific malforming. Following are the defined code points:

* Code = TBD9: Errored PDU. The BGP message was found to have some error that made it unusable, causing it to be treated-as-withdraw ~~RFC7606~~ [RFC7606].

3.3.4. Crossed Warning Bound TLV

TBD6 = Crossed Warning Bound TLV. The length is to be set to 4 bytes and the value to the threshold number of the event.

3.3.5. Crossed Upper Bound TLV

TBD7 = Crossed Upper Bound TLV. The length is to be set to 4 bytes and the value to the threshold number of the event.

3.4. Group TLV

The Group TLV is to form N:M relationships among NLRIs in the BGP Update PDU and TLVs of the same Route Event Logging message. This TLV has code point TBD4 and follows the definition of Group TLV in ~~TLV support for BMP Route Monitoring and Peer Down Messages~~ [I-D.ietf-grow-bmp-tlv].

3.5. Stateless Parsing TLV

The Stateless Parsing TLV is to allow parsing of the BGP Update PDU independently from a Peer Up message previously received for the same BGP session. This TLV can be especially relevant to Route Event Logging where the BGP Update PDU is artificial. The TLV has code point TBD5~~—~~, it follows the definition of Stateless Parsing TLV in ~~TLV support for BMP Route Monitoring and Peer Down Messages~~ [I-D.ietf-grow-bmp-tlv] and uses code point definitions in the

Commenté [MB14]: How to demux validation vs. malformed? Malformed can be seen as falling under validation failure

Commenté [MB15]: Which bound?

Commenté [MB16]: I would avoid depending on this one.

a mis en forme : Surlignage

a mis en forme : Surlignage

Commenté [MB17]: How is different from the previous code?

a mis en forme : Surlignage

Stateless Parsing Registry.

4. Operational Considerations

Route Event Logging messages are event-driven in nature so the general recommendation is to use them to report on specific conditions of interest in order, for example, to facilitate data mining or avoid differential analysis. When the objective is to annotate every received or announced NLRI then the recommendation is to use Route Monitoring messages with BMP Path Marking [I-D.ietf-grow-bmp-path-marking-tlv]. As an example, consider RPKI validation status: when the objective is to report on any validations tatus (i.e., valid, invalid and unknown), BMP Path Marking should be used; when the objective is instead to report only invalids then Route Event Logging with Validation Fail Event Reason should be used.

There ~~exist~~exists a definite overlap between Route Event Logging when used to report Malformed Packet and the use-cases for Route Mirroring where Errored PDUs may be sampled for reporting. From implementors perspective, if one wants to implement broader event-driven notifications and does not want to offer exact mirroring of monitored BGP sessions without state compression it may be ~~adviceable~~advisable to prefer implementing Route Event Logging message type over Route Mirroring. From a collector perspective, similarly, one may want to activate distinct BMP feeds for event logging and route collection and, also in this case, reporting malformed packets via Route Event Logging message type may be preferrable over Route Mirroring.

Crossed warning bound and crossed upper bound events refer to the received route thresholds that can be configured according to Section 6.7 of [RFC4271]. Also, the stats counters part of these events ~~is~~ are being addressed by the Definition For New BMP Statistics Type [I-D.ietf-grow-bmp-bgp-rib-stats] ~~document~~.

5. Security Considerations

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

6. IANA Considerations

TBD

7. References

[I-D.ietf-grow-bmp-bgp-rib-stats]
Srivastava, M., Liu, Y., Lin, C., and J. Li, "Definition For New BMP Statistics Type", Work in Progress, Internet-Draft, draft-ietf-grow-bmp-bgp-rib-stats-03, 8 May 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-bmp-bgp-rib-stats-03>.

[I-D.ietf-grow-bmp-path-marking-tlv]
Cardona, C., Lucente, P., Francois, P., Gu, Y., and T. Graf, "BMP Extension for Path Status TLV", Work in Progress, Internet-Draft, draft-ietf-grow-bmp-path-

Commenté [MB18]: Add a pointer

Commenté [BMI19]: Should there be some guard to rate-limit such messages?

Commenté [BMI20]: Can this be configured?

Commenté [BMI21]: I guess we should at least remind base 7854. Also, I wonder whether there is a risk of overload when abnormal events are observed which may lead to a large volume or RELs. Some rate limit guards maye be needed.

marking-tlv-01, 18 March 2024,
<https://datatracker.ietf.org/doc/html/draft-ietf-grow-bmp-path-marking-tlv-01>.

[I-D.ietf-grow-bmp-tlv]
Lucente, P. and Y. Gu, "BMP v4: TLV support for BMP Route Monitoring and Peer Down Messages", Work in Progress, Internet-Draft, draft-ietf-grow-bmp-tlv-14, 18 March 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-bmp-tlv-14>.

[I-D.ietf-grow-bmp-tlv-ebit]
Lucente, P. and Y. Gu, "Support for Enterprise-specific TLVs in the BGP Monitoring Protocol", Work in Progress, Internet-Draft, draft-ietf-grow-bmp-tlv-ebit-05, 18 March 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-bmp-tlv-ebit-05>.

[I-D.ietf-idr-bgp-model]
Jethanandani, M., Patel, K., Hares, S., and J. Haas, "YANG Model for Border Gateway Protocol (BGP-4)", Work in Progress, Internet-Draft, draft-ietf-idr-bgp-model-17, 5 July 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-idr-bgp-model-17>.

[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>.

[RFC7606] Chen, E., Ed., Scudder, J., Ed., Mohapatra, P., and K. Patel, "Revised Error Handling for BGP UPDATE Messages", RFC 7606, DOI 10.17487/RFC7606, August 2015, <https://www.rfc-editor.org/info/rfc7606>.

[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>.

[RFC8671] Evens, T., Bayraktar, S., Lucente, P., Mi, P., and S. Zhuang, "Support for Adj-RIB-Out in the BGP Monitoring Protocol (BMP)", RFC 8671, DOI 10.17487/RFC8671, November 2019, <https://www.rfc-editor.org/info/rfc8671>.

[RFC9067] Qu, Y., Tantsura, J., Lindem, A., and X. Liu, "A YANG Data Model for Routing Policy", RFC 9067, DOI 10.17487/RFC9067, October 2021, <https://www.rfc-editor.org/info/rfc9067>.

[RFC9069] Evens, T., Bayraktar, S., Bhardwaj, M., and P. Lucente, "Support for Local RIB in the BGP Monitoring Protocol (BMP)", RFC 9069, DOI 10.17487/RFC9069, February 2022, <https://www.rfc-editor.org/info/rfc9069>.

Acknowledgements

The authors would like to thank Jeff Haas, Luuk Hendriks, Ruediger Volk, Ahmed Elhassany, Thomas Graf, and Ben Maddison for their valuable input. The authors would also like to thank Mike Booth for his review.

Authors' Addresses

Paolo Lucente
NTT
Veemweg 23
3771 Barneveld
Netherlands
Email: paolo@ntt.net

Camilo Cardona
NTT
164-168, Carrer de Numancia
08029 Barcelona
Spain
Email: camilo@ntt.net