GROW
Internet-Draft
Intended status: Informational
Expires: 3 January 2026

S. Wang
M. Xu
Y. Wang
J. Zhang
Beijing Zhongguancun Laboratory

2 July 2025

Requirements for Monitoring RPKI-Related Processes on Routers Using BMP
draft-wang-grow-bmp-rpki-mon-reqs-01

Abstract

This document outlines requirements for extending the BGP Monitoring Protocol (BMP) to provide comprehensive monitoring of RPKI-related processes on routers on routers, including data retrieval from RPKI caches, RPKI-related policy configuration, route validation, and the impact of validation on routing decisions. The proposed extensions aim to standardize router-side monitoring on RPKI within BMP, addressing scalability and interoperability limitations in existing implementations.

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 3 January 2026.

Table of Contents

1. Introduction

The Resource Public Key Infrastructure (RPKI) enhances BGP security by enabling cryptographic validation of route origins [RFC6483] [RFC6811] and AS paths [I-D.ietf-sidrops-aspa-verification]. Despite growing adoption of RPKI, standard implementations of the BGP Monitoring Protocol (BMP) [RFC7854] do not natively support monitoring of RPKI-related data. This limitation hampers visibility into RPKI validation processes and their impact on network operations.

While existing proposals aim to extend BMP for specific aspects of RPKI monitoring—such as reporting invalid routes [I-D.ietf-grow-bmp-path-marking-tlv] [I-D.ietf-grow-bmp-rel] or providing validation statistics [I-D.ietf-grow-bmp-bgp-rib-stats]—they fall short of offering comprehensive, end-to-end monitoring of the RPKI lifecycle on routers. This document defines requirements and extensions for BMP to monitor four key stages:

* Retrieval of RPKI data from caches;

* Configuration of RPKI policies;

* Validation of routes using RPKI;

* Impact of RPKI validation on routing decisions.

2. 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].

3. Requirements Overview

The BMP extension for RPKI monitoring SHOULD:

* Monitor extensible RPKI data transport from caches to routers [RFC8210];

* Enable real-time monitoring of the route validation process on the router [RFC6811];

* Facilitate the correlation between RPKI validation states and BGP routing decisions;

* Scale efficiently across diverse validation types.

Consequently, this document identifies four key stages in the RPKI lifecycle on routers which necessitate detailed monitoring and reporting:

3.1. RPKI Data Retrieval from Caches

To ensure accurate and timely retrieval of RPKI data from caches, router operators require BMP to provide real-time, consistent monitoring on the health of RPKI cache connection. This enables rapid detection and response to faults or outages in cache connectivity. Accordingly, BMP SHOULD report the RTR connection parameters, the synchronization states, and error metrics.

3.2. RPKI Policy Configuration

Routing policies on the router may change dynamically, necessitating real-time monitoring to ensure correct implementation of RPKI-based policies and prompt detection of misconfigurations. To achieve this, BMP SHOULD report global RPKI enforcement status, and RPKI-related validation rules and actions for each peer.

3.3. Route Validation with RPKI

Routers from different vendors implement RPKI-based route validation— including origin validation and path validation —with varying approaches. To facilitate accurate troubleshooting against validation outcomes, BMP SHOULD report the RPKI validation state as well as the proof that contributes to the state.

3.4. Impact of RPKI Validation on Routing

A router may implement numerous routing policies, resulting in complex routing behavior that obscures the influence of RPKI validation on decision-making. To provide visibility into this impact, BMP should report both intended outcomes and unintended side effects that are caused by the RPKI validation process.

4. RPKI Data Retrieval from Caches

BMP SHOULD enumerate all RTR connections on the monitored router. For each RTR connection, BMP SHOULD report the following fields:

* The RPKI cache’s designation as primary or backup, including its priority in the selection order;
* The version of the RTR protocol in use (e.g., version 0 [RFC6810], version 1 [RFC8210], or custom versions);
* The type of TCP connection established (e.g., plain TCP, TLS, SSH);
* The IP address and port number of the cache;
* The total number of RPKI records received, including ROAs and ASPAs;
* The current status of the connection (e.g., active or idle);
* The timestamp of the most recent synchronization;
* Counters for errors and timeouts encountered;
* Any other relevant information.

To convey this information, a new BMP message type **RPKI_CONNECTION_REPORT** (Type = TBD1) SHOULD be defined. This message SHALL use the standard BMP common header followed by Type-Length-Value (TLV) elements per [I-D.ietf-grow-bmp-tlv]. For routers connected to multiple caches, TLVs SHALL be grouped per RTR

connection. Each group SHALL use a Group TLV to index Stateless parsing TLVs containing the above fields, thereby ensuring consistency and scalability.

5. RPKI Policy Configuration

BMP SHOULD report the RPKI-related policy configuration, which may be applied globally (uniformly applied across all peers) or on a per-peer basis (For example, only applied to the provider). The reported information SHOULD include:

* The enablement status of RPKI validation;

* If enabled, the complete set of validation rules derived from RPKI data, such as VRPs or ASPA entries;

* If enabled, the configured actions for routes determined to be in Invalid or Not-Found states.

To convey this information, a new BMP message type **RPKI_POLICY_REPORT** (Type = TBD2) SHOULD be defined. For global policy configurations, this message SHALL comprise the BMP common header followed by TLVs that specify the validation rules and the actions associated with each non-valid state (i.e., Invalid and Not-Found), such as filtering, priority reduction, tagging, or no action. For per-peer policy configurations, the message SHALL include an additional per-peer header, followed by TLVs that detail the RPKI policies specific to each peer.

6. Route Validation with RPKI

BMP SHOULD be extended to report both statistical summaries of validation results on a per-peer basis and detailed validation information for each route. For each peer, BMP messages SHOULD include counts of received routes categorized by their RPKI validation states. Existing proposals, such as [I-D.ietf-grow-bmp-bgp-rib-stats], recommend extending the BMP Statistics Report Message with new Stat Type codes to accommodate RPKI-related statistics.

However, to improve clarity and emphasize RPKI-specific data, it is RECOMMENDED that a dedicated **RPKI Statistics Section** be introduced within the BMP Statistics Report Message. This section SHOULD comprise predefined Stat Type TLVs for:

* The number of routes in each validation state: Valid, Invalid, and Not-Found;

* Optional statistics, such as the number of routes filtered as a result of RPKI validation.

This separation enhances readability and facilitates future extensions for additional RPKI-related statistics, such as those pertaining to ASPA or BGPsec.

For any individual route, BMP SHOULD report the validation state along with the specific reasons that led to that state. For instance:

* For Invalid routes, the message SHOULD include the relevant ROA or ASPA entry that caused the invalidation, detailing reasons such as a mismatch in the origin AS, a prefix length exceeding the ROA's maxLength, or an AS path that violates ASPA rules;

* For Not-Found routes, the message SHOULD indicate the absence of a corresponding ROA or other factors resulting in this state.

For per-route validation report, existing drafts propose extending BMP by:

* Incorporating additional path TLVs into the Route Monitoring Message for invalid routes [I-D.ietf-grow-bmp-path-marking-tlv];

* Defining a new Route Event Message type [I-D.ietf-grow-bmp-rel], where the emergence of invalid routes is treated as a distinct event.

To provide comprehensive report of RPKI validation for all routes, it is RECOMMENDED that a dedicated Validation Report Message **RPKI_VALIDATION_REPORT** (Type = TBD3) be defined. This message SHOULD contain TLVs that specify:

* The route's validation state;

* The relevant ROA or other validation records (like ASPAs);

* The rationale behind the validation decision, such as a mismatch in origin AS, an invalid prefix length, or the absence of a valid ROA.

7. Impact of RPKI Validation on Routing

BMP SHOULD report the consequences of RPKI validation on route selection, with a particular focus on routes whose selection status is altered by RPKI validation:

* Routes that are demoted due to RPKI validation (i.e., routes that would have been selected as the best path without RPKI but are not selected when RPKI is enabled);

* Routes that are promoted due to RPKI validation (i.e., routes that would not have been selected as the best path without RPKI but are selected when RPKI is enabled).

For each route affected by RPKI validation, the BMP extension SHOULD report:

* The validation information, as detailed in the Route Validation stage;

* The actions applied to the route following validation, such as degradation of preference, attribute tagging, or exclusion from the selection process.

Furthermore, the BMP message MAY include information about the alternate best route:

* For routes demoted due to RPKI, the message MAY report the new best route selected with RPKI enabled;

* For routes promoted due to RPKI, the message MAY report the best route that would have been selected without RPKI.

This facilitates a direct comparison of routing decisions with and without RPKI, thereby enhancing the understanding of RPKI’s influence on BGP path selection.

To enable per-route reporting of RPKI’s impact on BGP routing, the BMP extension can utilize the event-driven messaging mode proposed in [I-D.ietf-grow-bmp-rel]. A new Reason code **RPKI_IMPACT** (TBD4) SHOULD be defined for the Route Event Message, to capture changes in route handling due to RPKI validation and policies. When a route’s treatment is altered due to RPKI—such as being dropped, deprioritized, or superseded by another route—an RPKI-related event SHOULD be generated and conveyed via a Route Event Message. This message SHOULD include:

* The prefix and attributes of the affected route;

* The RPKI validation state of the affected route;

* Details of the RPKI validation, including the relevant ROA or ASPA;

* The policy action enforced on the route (e.g., drop, reduce priority, tag);

* Information regarding the new best route selected, including its prefix, attributes, and RPKI validation state.

8. Security Considerations

8.1. Transmission Security

To ensure the integrity and authenticity of the transmitted monitoring data on RPKI, BMP MUST support the following requirements:

* Protocol safety: BMP MUST employ either TCP Authentication Option (TCP-AO) [RFC5925] or Transport Layer Security (TLS) to encrypt the monitoring sessions.

* data integrity: BMP should enforce mechanism like end-to-end signatures to ensure the integrity of critical data such as ROA validation result fields and AS_PATH change records, and validate the integrity of the received data prior to extracting the content of the data to prevent the propagation of tampered or corrupted information. The signing/verification keys could be dynamically derived from the RPKI certificate authority chain or managed through other secure mechanisms, and form a cross-verification mechanism with the source AS validation results of BGP UPDATE messages (where applicable) to prevent malicious rollback or tampering of the related monitoring data during transmission.

8.2. Operational Security

To ensure the extended BMP aligns with router’s original configuration, BMP MUST support the followign requirements:

* Protocol transparency: The monitoring data collection must strictly adhere to the "zero-intrusion" principle. For operations involving the RTR protocol [RFC8210], only read-only interfaces are permitted to retrieve certificate synchronization status, and any modification to the router’s local RPKI cache tree structure is prohibited. The polling frequency of monitoring probes should be restricted, and appropriate memory access layer protections must be implemented to prevent cache reconstruction triggered by monitoring data extraction. Additionally, the acquisition of collected ROA validation records should not interfere with real-time traffic processing.

* Forward compatibility: When the router does not enable the monitoring function recommended by this standard, or when the monitoring function fails, its native RPKI validation process [RFC6811] and BGP decision logic must maintain full functional consistency to prevent unintended routing policy changes caused by the monitoring mechanism.

9. IANA Considerations

This document requires IANA to assign values for new BMP message types (TBD1-TBD3), reason code (TBD4) and their associated TLVs. The registration procedures for these assignments SHALL follow the policy outlined in [RFC7854].

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>.

[RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, DOI 10.17487/RFC5925, June 2010, <https://www.rfc-editor.org/info/rfc5925>.

[I-D.ietf-sidrops-aspa-verification] Azimov, A., Bogomazov, E., Bush, R., Patel, K., Snijders, J., and K. Sriram, "BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-verification-19, 27 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-19>.

[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>.

[RFC6483] Huston, G. and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)", RFC 6483, DOI 10.17487/RFC6483, February 2012, <https://www.rfc-editor.org/info/rfc6483>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2012, <https://www.rfc-editor.org/info/rfc6811>.

[RFC6810] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol", RFC 6810, DOI 10.17487/RFC6810, January 2013, <https://www.rfc-editor.org/info/rfc6810>.

[RFC8210] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1", RFC 8210, DOI 10.17487/RFC8210, September 2017, <https://www.rfc-editor.org/info/rfc8210>.

[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-15, 17 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-bmp-tlv-15>.

10.2. Informative References

[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-marking-tlv-02, 16 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-bmp-path-marking-tlv-02>.

[I-D.ietf-grow-bmp-rel] Lucente, P. and C. Cardona, "Logging of routing events in BGP Monitoring Protocol (BMP)", Work in Progress, Internet-Draft, draft-ietf-grow-bmp-rel-02, 8 July 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-bmp-rel-02>.

[I-D.ietf-grow-bmp-bgp-rib-stats] Srivastava, M., Liu, Y., Lin, C., and J. Li, "Definition For New BGP Monitoring Protocol (BMP) Statistics Types", Work in Progress, Internet-Draft, draft-ietf-grow-bmp-bgp-rib-stats-07, 21 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-grow-bmp-bgp-rib-stats-07>.

Authors' Addresses

Shuhe Wang
Beijing Zhongguancun Laboratory
Building 8, CourtYard 1, Zhongguancun East Road, Haidian District
Beijing
China
Email: wangsh@mail.zgclab.edu.cn

Mingwei Xu
Beijing Zhongguancun Laboratory
Building 8, CourtYard 1, Zhongguancun East Road, Haidian District
Beijing
China
Email: xmw@cernet.edu.cn

Yangyang Wang
Beijing Zhongguancun Laboratory
Building 8, CourtYard 1, Zhongguancun East Road, Haidian District
Beijing
China
Email: wyy@cernet.edu.cn

Jia Zhang
Beijing Zhongguancun Laboratory
Building 8, CourtYard 1, Zhongguancun East Road, Haidian District
Beijing
China
Email: zhangj@mail.zgclab.edu.cn