RPKI-based Validation with Prioritized Resource Data

Abstract

Based on RPKI ROAs, Route Origin Validation (ROV) is a practical solution to address prefix origin hijacking. During ROV operations, the data used may come from local sources other than ROAs. These data sources can vary in terms of credibility, and ROV operations may require different response actions for invalid or unknown routes. This document describe an enhancement of ROV with multi-level priority, and outlines the use cases, framework, and requirements for ROV operations that involve multi-level priority.

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 14 April 2026.

Copyright Notice

Table of Contents

1. Introduction

Route Origin Validation (ROV), which is built on RPKI Route Origin Authorizations (ROAs), stands as a practical and effective approach to combat prefix origin hijacking. In ROV operations, the validating data utilized is not limited to ROAs alone; it may also include various types of local data from other sources. These additional data sources can exhibit varying levels of credibility, with some being highly reliable due to their authoritative origins and others being less trustworthy due to potential inconsistencies or lack of verification. Correspondingly, ROV operations need to be flexible enough to take different actions when dealing with invalid routes

and unknown routes. This document introduces an enhancement of ROV with multi-level priority, and elaborates the gap analysis, framework, and specify the key requirements for implementing ROV with multi-level priority in current RPKI infrastructure.

1.1. Requirements Language

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.

2. Gap analysis

ROV (Route Origin Validation) based on RPKI (Resource Public Key Infrastructure) relies on ROA (Route Origin Authorization) data. It is known that ROA data has the following deployment issues: it does not fully cover all routes in the routing table; there exist ROA data with artificial registration errors; and network operators can filter specific validation data from VRP (Validated ROA Payload) data locally as needed, or supplement it with additional data (e.g., data inferred through machine learning). SLURM (Simplified Local Internet Number Resource Management) technology can be used to modify the data locally.

Due to such mixed data sources, the credibility of the data varies to different degrees and is no longer uniform. Similarly, network operators expect to perform different operations on validation results based on their credibility. This approach offers benefits such as the following use case: an ISP (Internet Service Provider) uses data derived from its own experience to supplement RPKI ROAs, but the credibility of this supplementary data is lower than that of RPKI ROAs. When a route is verified as "invalid" by RPKI ROAs, the router can discard the route; if a route is verified as "invalid" by supplementary data with medium credibility, the router can be configured to trigger an alert.

However, current RPKI technology does not support such operations. Regardless of the source of the validation data, the same type of validation result triggers the same operation. This fails to meet the need for customized processing of different scenarios in network operations. This document describes a RPKI validation mechanism with multi-level priority to make RPKI-based validation processing more flexible.

3. Framework

This document proposes a framework shown as the following figure. It sopports RPKI-based validation with prioritized resource data.

```
                +-----------------+
                | RP/Cache server |
                | +-------------+ |
                | | prioritized | |<-----RPKI data
                | | resource    | |<-----AI data
                | | data        | |<-----Locally
                | +-------------+ |        imported data
                +-----------------+
                  /             \
                 / RTR PDUs with \
                / priority levels \
               /                   \
  +-----------\/-----+        +------\/----------+
  |      Router      |        |      Router      |
  |+---------------+|        |+---------------+|
  ||route validation||        ||route validation||
  ||with prioritized||        ||with prioritized||
  ||resource data   ||        ||resource data   ||
  |+---------------+|        |+---------------+|
  +-----------------+        +-----------------+
```
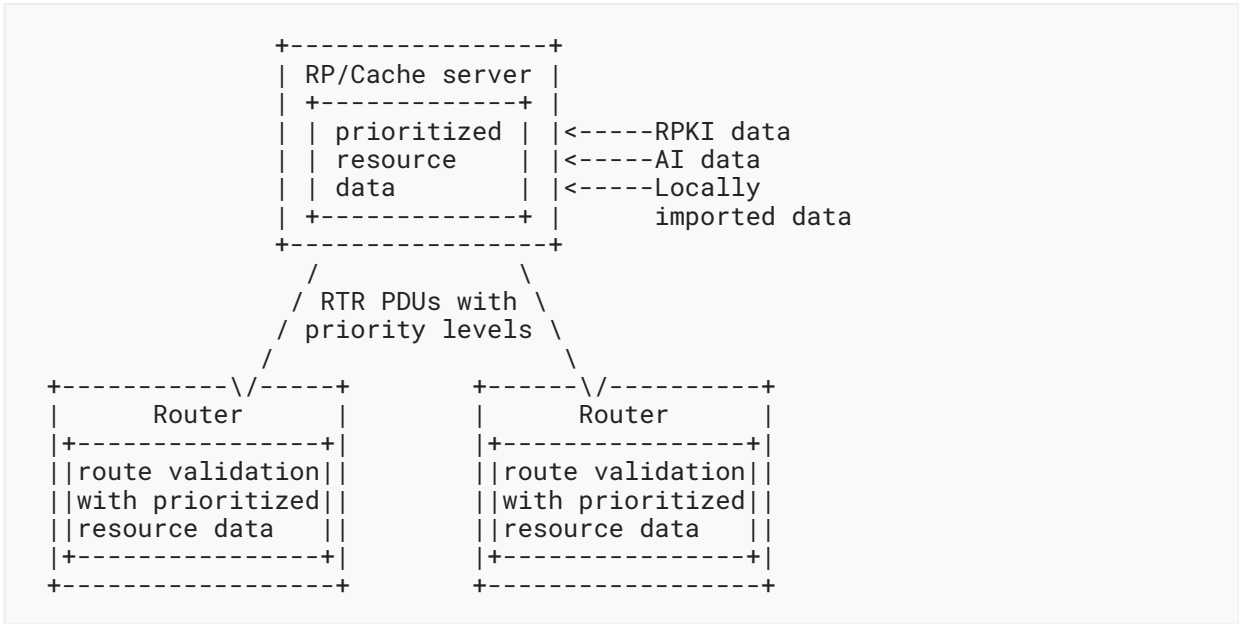
The RP/Cache server collects and manages resouce data (e.g., ROA/ASPA) which are from different sources such as RPKI repository, AI inference, and local import. The data from different sources will be set to different priorities. The RP/Cache server needs to decide how to merge these data from different sources.

The data will be syncronized from the RP/Cache server to routers through tools like RTR. Routers will do BGP route validation with priorities being taken into consideration. Particularly, the validaiton output for a route can be Valid, Unknown, or Invalid-*level*. A route validated as invalid will be marked with Invalid as well as a credibility level of the validation result. For example, "Invalid-*1*" means the validation result of invalid is derived based on the source data with the priority of *1* and thus has a credibility level of *1*.

Network operators can do configurations on routers to taken different policies on the invalid routes with different credibility levels. For example, suppose there are two ROA records on a router: 1) the prefix of 192.0.1.0/24 is authorized to AS 65001, which has a high priority of *1* and 2) the prefix of 192.0.2/24 is authorized to AS 65002, which has a relatively low priority of *2*. For the route with the prefix of 192.0.1.0/24 and the origin of AS 65003, the validation result will be invalid-*1*. Operators can configure the router to discard the route because the validation result is with a high credibility level. For the route with the prefix of 192.0.2.0/24 and the origin of AS 65003, the validation result will be invalid-*2*. Operators can choose to set a lower priority for this route to influence the route selection outcome. This is because the validation result is with a relatively low credibility level and adopting a conservative handling policy to the route may be safer.

The proposed framework brings two main benefits:

• Enhancing BGP route handling after route validation. When the resource data are from multiple data sources with different levels of credibility, operators can implement customized priority settings to the resource data and apply different handling policies.

• Improving early deployment benefits and promoting the deployment of RPKI-based routing validation techniques. When the registration rate of RPKI data is not high, operators can supplement data with techniques like AI while still being able to take "discarding" action on invalid routes with high credibility levels.

4.   Requirements for Multi-Priority RPKI ROV

This section outlines the requirements for extending the RPKI architecture to support the processing and propagation of RPKI data with multiple priority levels. These requirements are necessary to enable differentiated handling of routing validation results based on their perceived trustworthiness, such as those derived from authoritative sources (e.g., RPKI ROAs) versus inferred or supplemental sources (e.g., AI-generated data).

4.1. Priority Setting

Implementations processing RPKI data on local cache (e.g., Relying Party software) **MUST** support the assignment of a priority level to each validated RPKI object. The priority **SHOULD** be configurable based on the data source (e.g., RPKIsigned, locally imported, or AI-inferred). The priority value **MUST** be represented in a standardized format to ensure interoperability.

4.2. Multi-Priority Data Merge

Implementations **MUST** merge data from multiple sources according to a defined algorithm. This algorithm **SHOULD** specify how to handle conflicts, including rules for merging data of the same priority and for superseding lower-priority data with higher-priority data.

4.3. SLURM Support for Priority Marking

The SLURM mechanism **MUST** be extended to allow local exceptions and additions to include a priority attribute. This enables network operators to override or supplement RPKI data with local policies that reflect differentiated trust levels.

4.4. RTR Support for Priority Marking

The RPKI-to-Router (RTR) protocol **MUST** be extended to convey the assurance level (priority) of the validation data it delivers. This enables routers to apply appropriate local policy based on the trustworthiness of the origin. To provide flexibility in deployment, two implementation models **SHALL** be supported:

1. One single local cache server transmits data of multiple assurance levels. The protocol **MUST** be extended to include a new field within its Protocol Data Units (PDUs) to explicitly carry the assurance level for each payload data item (e.g., a ROA or an ASPA). This model allows a router to maintain a single, simple transport session with one cache server while receiving a mixedpriority data set.

2. A router establishes transport sessions with multiple local cache servers, where each server is designated to provide data for a specific assurance level (e.g., a primary server provides highpriority RPKI-validated data, and a secondary server provides low-priority supplemental data). The protocol itself remains unchanged, as the priority is derived from the configuration of the router-to-server association

Network operators **SHOULD** choose which implementation to deploy based on their specific operational preferences and infrastructure.

4.5. ROV/ASPA Validation with Priority Awareness

ROV and ASPA validation processes **MUST** be enhanced to support a multi-priority data model. The validation process **SHOULD** annotate the resulting validation state (Valid, Invalid) with an indication of the assurance level, which identifies the priority tier of the data that was used to reach that conclusion. For example, an "Invalid" result derived from a local override (high-priority) **MUST** be distinguishable from an "Invalid" result derived from inferred data (low-priority).

This annotated validation state **SHOULD** then be used to inform subsequent routing policy actions. Implementations **SHOULD** provide flexible policy mechanisms that allow network operators to define actions (e.g., reject, depreference, warn, accept) based on both the validation state (e.g., Invalid) and its associated assurance level (e.g., High or Low).

4.6. Router Handling of Priority-Based Invalid Routes

BGP speakers **SHOULD** support configurable policies to handle invalid routes based on the priority of the validation data. For example, routes invalidated by high-priority data **MAY** be deprioritized or discarded, while those invalidated by low-priority data **MAY** be retained with a warning.

4.7. BMP Support for Priority in Validation Reports

The BGP Monitoring Protocol (BMP) **SHOULD** be extended to include priority information in reports of ROV/ASPA validation results. This enables network operators to monitor and analyze routing decisions based on data trust levels.

5. Security Considerations

This document defines a framework for handling RPKI data with multiple levels of priority (assurance), which introduces new considerations beyond those of the base RPKI system [RFC6480].

Amplification of RPKI Repository Failures: If a high-priority source (e.g., a primary RTR cache) becomes stale or unavailable, the system may fall back to low-priority data. This could lead to a mass re-evaluation of routes from a 'Unknown' state to a 'Valid' or 'Invalid' state based on less

trustworthy information, potentially causing widespread routing churn. Implementations should include mechanisms to detect such scenarios and allow operators to define appropriate fallback behaviors.

6. IANA Considerations

This document has no IANA action.

7. References

7.1. 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>.

[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>.

7.2. Informative References

[RFC6480]   Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

Author's Address

XX XX
XXX
Beijing
China
Email: xx@sina.com