

Workgroup: SIDROPS Working Group
Internet-Draft:
draft-sriram-sidroops-drop-invalid-policy-10
Published: 27 November 2022
Intended Status: Best Current Practice
Expires: 31 May 2023
Authors: K. Sriram O. Borchert D. Montgomery
 USA NIST USA NIST USA NIST

Origin Validation Policy Considerations for Dropping Invalid Routes

Abstract

Deployment of Resource Public Key Infrastructure (RPKI) and Route Origin Authorizations (ROAs) is expected to occur gradually over several or many years. During the incremental deployment period, network operators would wish to have a meaningful policy for dropping Invalid routes. Their goal is to balance (A) dropping Invalid routes so hijacked routes can be eliminated, versus (B) tolerance for missing or erroneously created ROAs for customer prefixes. This document considers a Drop Invalid if Still Routable (DISR) policy that is based on these considerations. The key principle of DISR policy is that an Invalid route can be dropped if a Valid or NotFound route exists for a subsuming less specific prefix.

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 31 May 2023.

Copyright Notice

Copyright (c) 2022 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 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

- [1. Introduction](#)
- [2. Drop Invalid if Still Routable \(DISR\) Policy](#)
 - [2.1. Motivation for the DISR Policy](#)
- [3. Algorithm for Implementation of DISR Policy](#)
- [4. Security Considerations](#)
- [5. Normative References](#)
- [Acknowledgements](#)
- [Authors' Addresses](#)

1. Introduction

Deployment of Resource Public Key Infrastructure (RPKI) [[RFC6481](#)] and Route Origin Authorizations (ROAs) [[RFC6482](#)] is expected to occur gradually over several or many years. ROA-based BGP Origin Validation (OV) process and the OV states are defined in [[RFC6811](#)]. During the incremental deployment period, network operators would wish to have a meaningful policy for dropping Invalid routes. Their goal is to balance (A) dropping Invalid routes so hijacked routes can be eliminated, versus (B) tolerance for missing or erroneously created ROAs for customer prefixes. This document considers a Drop Invalid if Still Routable (DISR) policy that is based on these considerations. The key principle of DISR policy is that an Invalid route can be dropped if a Valid or NotFound route exists for a subsuming less specific prefix.

The DISR policy applies in addition to (1) preferring Valid when more than one route exists for the same prefix, and (2) always including NotFound routes in the best path selection process. Note that for a router performing OV, the existence of a NotFound route excludes the possibility of an alternate Valid or Invalid route for the same prefix or a subsuming less specific prefix.

This document also provides an algorithm for best path selection policy that considers Origin Validation (OV) outcome and includes the DISR policy.

2. Drop Invalid if Still Routable (DISR) Policy

When BGP origin validation (OV) [[RFC6811](#)] is performed on a BGP route, there are three possible outcomes: (1) Valid, (2) Invalid, or

(3) NotFound. During partial/incremental deployment of RPKI and ROAs, it is natural to always include Valid and NotFound routes in the path selection decision process. Note that Valid and NotFound are mutually exclusive, i.e., at a validating router, there cannot be two routes for a prefix where one is Valid and the other is NotFound. Similarly, Invalid and NotFound are also mutually exclusive. If Invalid routes are always dropped from consideration, then there would be no tolerance for missing or erroneously created ROAs for customer prefixes. Then the question arises whether the following policy should be considered: Drop an Invalid route only if another Valid or NotFound route exists for a subsuming less specific prefix? This policy is called Drop Invalid if Still Routable (DISR).

The existence of an AS0 ROA for a prefix means that the prefix or any more specific prefix subsumed in it are forbidden from routing except when there exists a different ROA with a normal ASN for the prefix or the more specific prefix. DISR policy MUST apply the following exception: If a route is Invalid due to an AS0 ROA, then always drop the route.

Any routes for 0.0.0.0/0 (IPv4) or ::/0 (IPv6) in the routing table must be excluded from consideration in the DISR policy. (Author's note: Think this through with help from the WG.)

2.1. Motivation for the DISR Policy

Consider these scenarios:

Scenario 1: A transit ISP A (AS A) created a ROA for a /22 prefix they announce. They also announce a /24 prefix (subsumed in the /22) that is owned by directly-connected customer X (has no AS). But ISP A neglected to create a ROA for X's /24 prefix. Clearly, the announcement of X's /24 will be Invalid. ISP A happens to propagate to neighbors the /22 and the /24.

Scenario 2: Customer X (AS X) announces a /22 prefix only to transit ISP A and a /24 prefix (subsumed in the /22) only to transit ISP B. X is attempting to do traffic engineering (TE). X created a ROA for the /22 but neglected to have ROA coverage for the /24. Clearly, X's announcement of the /24 will be Invalid. ISP B does not participate in OV and propagates the Invalid route to its neighbors.

In each of the above scenarios, DISR policy (applied at routers elsewhere in the Internet) ensures that traffic for the more specific (/24) still reaches the correct destination, i.e., customer X (albeit possibly via a suboptimal / non-TE path). Any actual hijacks of the /24 prefix would be dropped at all eBGP routers that employ the DISR policy. Please see [[sriram-disr](#)] for analysis of several more scenarios.

Measurements show that if OV were performed, there are 10,417 Invalid routes in the global Internet based on analysis of Routeviews/RPKI/ROA data from February 2018. Of these, 6846 routes are Invalid due to exceeding the maxlength. 6027 of the 6846 Invalid prefixes are seen to be routable via alternate Valid or NotFound routes for either the same prefix (as in the Invalid route) or a subsuming less specific prefix. Again, 5987 of the 6027 are routes for which the corresponding Valid or NotFound routes (with the same or subsuming less specific prefix) have the exact same origin AS as in the Invalid route in question. These measurements show that Scenarios 1 and 2 described above do occur in significant numbers currently. So, the data lends support to the efficacy of the DISR policy in terms of delivering the data traffic to the right destination though not necessarily via the optimal/TE path. Please see [[sriram-disr](#)] for more detailed results from the Routeviews/RPKI/ROA data measurement study.

The following is recommended in BCP 185 [[RFC7115](#)]: "Before issuing a ROA for a super-block, an operator MUST ensure that all sub-allocations from that block that are announced by other ASes, e.g., customers, have correct ROAs in the RPKI." However, as seen by the above measurement data, there are lapses in following this recommendation.

Network operators who do not wish to drop Invalid routes outright in partial deployment SHOULD consider employing the DISR policy. It helps eliminate actual prefix hijacks, while incentivizing creation of required ROAs and the adherence to the above recommendation from BCP 185. The stick used here is the possibility of data traveling via a suboptimal path, while the more aggressive stick of dropping all Invalid routes is held in abeyance.

3. Algorithm for Implementation of DISR Policy

An algorithm for implementation of the DISR policy is as follows.

Perform the following steps when a route is received:

1. Perform BGP Origin Validation (OV) [[RFC6811](#)] on the routes in the Adj-RIB-ins.
2. Apply best path decision process including the results of OV. Include NotFound routes in the decision process. When there is a choice, prefer Valid over Invalid routes.
3. Store the selected routes in the Loc-RIB.
4. Apply the DISR policy. Process routes in the order of least specific to most specific. If a selected route in the Loc-RIB is Valid/NotFound, then add the route to FIB and Adj-RIB-outs;

Else, if Invalid, then add the route to FIB and Adj-RIB-outs only if there is no existing Valid/NotFound route in the Loc-RIB for a subsuming Less Specific prefix.

Additional steps in the algorithm that are performed in reaction to addition/withdrawal of routes that influence DISR policy decisions and due to changes in RPKI:

- a. When a Valid/NotFound route is added to Loc-RIB, check if there are any more specific prefixes in the FIB and Adj-RIB-Outs subsumed by the route prefix; If such more specific prefix route is Invalid, then remove it from the FIB and Adj-RIB-Outs.
- b. When a Valid/NotFound route is withdrawn from Loc-RIB, check if there are any more specific prefixes in the Loc-RIB subsumed by the route prefix; If such more specific prefix route is Invalid, then add the route to FIB and Adj-RIB-outs.
- c. When the router is notified of RPKI state change, then list all the prefixes effected by it. Rerun route selection decision and DISR policy for those prefixes.

4. Security Considerations

This document addresses some aspects of best common practices for origin validation and related BGP policy. The security considerations provided in RFC 6811 [[RFC6811](#)] and BCP 185 [[RFC7115](#)] also apply here.

5. Normative References

- [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>>.
- [RFC6481] Huston, G., Loomans, R., and G. Michaelson, "A Profile for Resource Certificate Repository Structure", RFC 6481, DOI 10.17487/RFC6481, February 2012, <<https://www.rfc-editor.org/info/rfc6481>>.
- [RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <<https://www.rfc-editor.org/info/rfc6482>>.
- [RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <<https://www.rfc-editor.org/info/rfc6811>>.

[RFC7115]

Bush, R., "Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)", BCP 185, RFC 7115, DOI 10.17487/RFC7115, January 2014, <<https://www.rfc-editor.org/info/rfc7115>>.

[sriram-disr] Sriram et al., K., "Origin Validation Policy Considerations for Dropping Invalid Routes", Presented at the SIDROPS WG Meeting, IETF-101, London , March 2018, <<https://datatracker.ietf.org/meeting/101/materials/slides-101-sidrops-origin-validation-policy-considerations-for-dropping-invalid-routes-00>>.

Acknowledgements

The authors wish to thank Sebastian Spies, Saku Ytti, Jeffrey Haas, Tim Bruijnzeels, Keyur Patel, Warren Kumari, John Scudder, and Jay Borkenhagen for comments and discussion related to this work. Also, thanks are due to Lilia Hannachi for her insightful analysis of global RPKI and BGP data that has been helpful in this work.

Authors' Addresses

Kotikalapudi Sriram
USA National Institute of Standards and Technology

Email: ksriram@nist.gov

Oliver Borchert
USA National Institute of Standards and Technology

Email: oliver.borchert@nist.gov

Doug Montgomery
USA National Institute of Standards and Technology

Email: doug@nist.gov