Workgroup: SIDR Operations
Internet-Draft:
draft-ietf-sidrops-roa-considerations-02
Published: April 2022
Intended Status: Informational
Expires: 29 October 2022
Authors: Z. Yan R. Bush
CNNIC Internet Initiative Japan
G.G. Geng J. Yao
Jinan University CNNIC

Avoidance for ROA Containing Multiple IP Prefixes

Abstract

In RPKI, the address space holder needs to issue an ROA object when authorizing one or more ASes to originate routes to IP prefix(es). During ROA issurance process, the address space holder may need to specify an origin AS for a list of IP prefixes. Additionally, the address space holder is free to choose to put multiple prefixes into a single ROA or issue separate ROAs for each prefix according to the current specification. This memo analyzes some operational problems which may arise from ROAs containing multiple IP prefixes and recommends avoiding placing multiple IP prefixes in one ROA.

Status of This Memo

This Internet-Draft will expire on 3 October 2022.

Copyright Notice

Table of Contents

1. Introduction

In Resource Public Key Infrastructure (RPKI), Route Origin Authorization (ROA) is a digitally signed object which identifies that a single AS has been authorized by the address space holder to originate routes to one or more prefixes within the address space[RFC6482].

Each ROA contains an "asID" field and an "ipAddrBlocks" field. The "asID" field contains one single AS number which is authorized to originate routes to the given IP address prefixes. The "ipAddrBlocks" field contains one or more IP address prefixes to which the AS is authorized to originate the routes. If the address space holder needs to authorize more than one ASes to advertise the same set of address prefixes, the holder must issue multiple ROAs, one for each AS number. However, at present there are no mandatory requirements describing that the address space holders must issue a separate ROA for each prefix or a ROA containing multiple prefixes.

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. Problem statement and Analysis

Currently, there are about 24% ROAs containing two or more prefixes. Among them, the average number of prefixes per ROA exceeds 10.

For ROAs containing multiple prefixes, adding or deleting one <AS, ip_prefix> pair, the entire ROA must be withdrawn and reissued, or covered by a new ROA. That is, although aggregating multiple IP prefixes can reduce the number of issued ROA, updating an ROA containing multiple IP address prefixes will result in redundant transmission between RP and BGP routers because in reality just the changed IP prefix needs to be updated by the new ROA. Updating these ROAs frequently will increase the convergence time of BGP routers and reduce the stability of RPKI and BGP system.

In addition, ROAs have a long validity period in default, during which the prefix ownership is more likely to change (of course, resource shrink may happen at any time), which will lead to the withdrawal or reissue of the whole set of prefixes aggregated within the same ROA. This will increase the mis-configuration possibility and operational complexity [RFC8211]. If one prefix is included in the list by mistake, the whole ROA will not be generated successfully.

4. Suggestions

The following suggestions should be considered during the process of ROA issurance:

1) It's the most important to guarantee the stability and security of RPKI and BGP system, and it is recommended to include a single IP prefix in each ROA in default.

2) In some special scenarios, where the resource is very stable or a CA has operational problems producing increased number of individual ROAs, multiple IP prefixes may be aggregated in one ROA.

5. Security Considerations

This memo does not give rise to additional security risks.

6. IANA Considerations

This document does not request any IANA action.

7. Acknowledgements

The authors would like to thanks the valuable comments made by members of sidrops WG and the list will be updated later.

This work was supported by the Beijing Nova Program of Science and Technology under grant Z191100001119113.

This document was produced using the xml2rfc tool [RFC2629].

8. References

8.1. 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>.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, DOI 10.17487/RFC2629, June 1999, <https://www.rfc-editor.org/info/rfc2629>.

[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>.

8.2. Informative References

[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>.

[RFC8211] Kent, S. and D. Ma, "Adverse Actions by a Certification Authority (CA) or Repository Manager in the Resource Public Key Infrastructure (RPKI)", RFC 8211, DOI 10.17487/RFC8211, September 2017, <https://www.rfc-editor.org/info/rfc8211>.

Appendix A. ROA Analysis

In order to illustrate the situations of the current ROA database, the following analysis is made.

The total number of ROAs	The number of ROAs with a single prefix	The number of ROAs with multiple prefixes
105542	81759	23783

Figure 1: Statistical results of global ROAs

As shown in Figure. 1, by April 24th 2022, the total number of ROA objects issued is about 105542. Based on the further analysis on these ROA objects, it is found that the number of ROAs containing only one prefix is about 81759 (77.47% of all ROA objects), and the number of ROAs containing two or more prefixes is about 23783 (22.53% of all ROA objects).

In the 23783 ROA objects which each one contains two or more prefixes, the number of IP address prefixes are calculated and analyzed. The statistical results are shown in Figure. 2.

The number of prefixes	The number of ROAs	The average number of prefixes in each ROA
248693	23783	10.46

Figure 2: Statistical results of the ROAs with multiple prefixes

As described in Figure. 2, there are 248693 IP address prefixes in the 23783 ROA objects. And the average number of prefixes in each ROA is 10.46 (248693/23783). In addition, four types of ROAs are analyzed and calculated within the 23783 ROAs: ROAs each contains 2-10/11-50/51-100/>100 IP address prefixes. The statistical results are presented in Figure. 3.

ROA types	ROA with 2-10 prefixes	ROA with 11-50 prefixes	ROA with 51-100 prefixes	ROA with >100 prefixes	Total number
The number of ROAs	20286	2880	322	295	23783
The ratio of ROAs	85.30%	12.11%	1.35%	1.24%	100%
The number of prefixes	74504	59015	22244	92930	248693
The ratio of prefixes	29.96%	23.73%	8.94%	37.37%	100%

Figure 3: Statistical results of four types of ROAs

As shown in Figure. 3, taking the first type of ROA as an example, there are 20286 ROAs (85.3% of the 23783 ROA objects) which each contains 2-10 IP address prefixes, and the total number of IP prefixes in these 20286 ROAs is 74504 (29.96% of the 248693 prefixes).

It shows that the address space holders tend to issue each ROA object with fewer IP prefixes (more than 95% of ROAs containing less than 50 prefixes), but they still tend to put multiple prefixes into one single ROA.

The longest and shortest validity periods of a single ROA is 28854 days and 2 days. In addition, the average validity period of each ROA is 707.83 days.

Authors' Addresses

Zhiwei Yan
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing, 100190
P.R. China

Email: yanzhiwei@cnnic.cn

Randy Bush
Internet Initiative Japan

Email: randy@psg.com

Guanggang Geng
Jinan University
No.601, West Huangpu Avenue
Guangzhou
510632
China

Email: gggeng@jnu.edu.cn

Jiankang Yao
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing, 100190
P.R. China

Email: yaojk@cnnic.cn