SIDR Operations
Internet-Draft
Intended status: Informational
Expires: September 30, 2020

Z. Yan
CNNIC
R. Bush
Internet Initiative Japan
G. Geng
J. Yao
CNNIC

March 29, 2020

# Problem Statement and Considerations for ROAs issued with Multiple Prefixes
## draft-yan-sidrops-roa-considerations-04

Abstract

The address space holder needs to issue an ROA object when it authorizes one or more ASes to originate routes to multiple prefixes. During the process of ROA issuance, the address space holder needs to specify an origin AS for a list of IP prefixes. Besides, the address space holder has a free choice to put multiple prefixes into a single ROA or issue separate ROAs for each prefix based on the current specification. This memo analyzes and presents some operational problems which may be caused by the misconfigurations of ROAs containing multiple IP prefixes. Some suggestions and considerations also have been proposed.

Table of Contents



## 1. Introduction

Route Origin Authorization (ROA) is a digitally signed object which is used to identify 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].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 per AS number. However, at present there are no mandatory requirements in any RFCs describing that the address space holders must issue a separate ROA for each prefix or a ROA for multiple prefixes.

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. The ROAs with multiple prefixes is a common case that each ROA contains exactly one

AS number but may contain multiple IP address prefixes in the operational process of ROA issuance.

## 2. Terminology

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. Problem statement and Analysis

As mentioned above, the address space holder needs to issue an ROA object when it authorizes one or more ASes to originate routes to multiple prefixes. During the process of ROA issuance, the address space holder needs to specify an origin AS for a list of IP prefixes. Besides, the address space holder has a free choice to put multiple prefixes into a single ROA or issue separate ROAs for each prefix based on the current specification.

In reality, the address space holders tend to issue each ROA object with fewer IP prefixes, but they still tend to put multiple prefixes into one single ROA.

A large number of experiments for the process of ROA issuance have been made on our RPKI testbed, it is found that the misconfigurations during the issuance may cause the ROAs which have been issued to be revoked.

Another potential influence of misconfigurations of ROAs containing multiple IP prefixes on BGP routers may be considered. For the ROA containing multiple prefixes, once increase or delete one <AS, ip_prefix> pair in it, this ROA will be reissued. Through sychronization with repository, RPs fetch a new ROA object and then notify and send all the <AS, ip_prefix> pairs in this ROA to BGP routers. That is to say, the update of the ROA containing multiple IP address prefixes will lead to redundant transmission between RP and BGP routers . So frequent update of these ROAs will increase the convergency time of BGP routers and reduce their performance obviously.

## 4. Suggestions and Considerations

Based on the statistical and experimental analysis, following suggestions should be considered during the process of ROA issuance:

1) The issuance of ROAs containing a large number of IP prefixes may lead to misconfigurations more easily than ROAs with fewer IP prefixes.

A ROA which contains a large number of IP prefixes is more vulnerable to misconfigurations, because any misconfiguration of these prefixes may cause the legitimate ROA to be revoked. Besides, since the misconfigurations of ROAs containing a larger number of IP address prefixes may lead to much more serious consequences (a large-scale network interruption) than ROAs with fewer IP address prefixes, it is suggested to avoid issuing ROAs with a large number of IP address prefixes.

2) The number of ROAs containing multiple IP prefixes should be limited and the number of IP prefixes in each ROA should also be limited.

The extreme case (a single ROA can only contain one IP address prefix) may lead to too many ROA objects globally, which may in turn become a burden for RPs to synchronize and validate all these ROA objects with the fully deployment of RPKI. So a tradeoff between the number of ROAs and the number of IP prefixes in a single ROA should be considered.

3) A safeguard scheme is essential to protect the process of ROA issuance

Considering the misconfigurations during the process of ROA issuance are inevitable and the serious consequences they may lead to, a safeguard scheme to protect and monitor the process of ROA issuance should be considered.

## 5. Security Considerations

TBD.

## 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.

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>.

[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>.

### 8.2. Informative References

[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>.

## Appendix A. Acknowledgments

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

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

Email: gengguanggang@cnnic.cn

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

Email: yaojk@cnnic.cn