Problem Statement and Considerations for ROAs issued with Multiple Prefixes

draft-yan-sidrops-roa-considerations

@IETF 100 SIDROPS meeting

CNNIC

Background—RFC 6482

A ROA is a digitally signed object that provides a means of verifying that an IP address block holder has authorized an Autonomous System (AS) to originate routes to one or more prefixes within the address block.

ROAs are digitally signed objects that bind an address to an AS number, and are signed by the address holder.

```
RouteOriginAttestation ::= SEQUENCE {
   version [0] INTEGER DEFAULT 0,
   asID  ASID,
   ipAddrBlocks SEQUENCE (SIZE(1..MAX)) OF ROAIPAddressFamily }
```

The content of a ROA identifies a single AS that has been authorized by the address space holder to originate routes and a list of one or more IP address prefixes that will be advertised.
If the address space holder needs to authorize multiple ASes to advertise the same set of address prefixes, the holder issues multiple ROAs, one per AS number.

```
ASID ::= INTEGER

ROAIPAddressFamily ::= SEQUENCE {
   addressFamily OCTET STRING (SIZE (2..3)),
   addresses SEQUENCE (SIZE (1..MAX)) OF ROAIPAddress }

ROAIPAddress ::= SEQUENCE {
   address IPAddress,
   maxLength INTEGER OPTIONAL }

IPAddress ::= BIT STRING
```

ROAs issued with Multiple Prefixes

- What are the ROAs issued 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.

Statistical analysis

- By the July 4, 2017, the total number of ROA objects issued around the world is about 7166. the number of ROAs containing only one prefix is about 3307 (account for 46.1% of all ROA objects), and the number of ROAs containing two or more prefixes is about 3859 (account for 53.9% of all ROA objects).

The total number of ROAs	The number of ROAs with a single prefix	The number of ROAs with multiple prefixes
7166	3307	3859

Statistical analysis

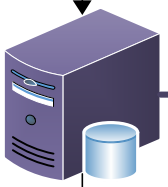
- There are 37367 IP address prefixes in the 3859 ROA objects. And the average number of prefixes in each ROA is 9.68

ROA types	Number of ROAs	ratio of ROAs	Number of prefixes	ratio of prefixes
ROA with 2-10 prefixes	3263	84.56%	12442	33.30%
ROA with 11-50 prefixes	496	12.85%	10365	27.74%
ROA with 51-100 prefixes	60	1.55%	4125	11.04%
ROA with >100 prefixes	40	1.04%	10435	27.92%
Total	3859	100.00%	37367	100.00%

Experimental analysis

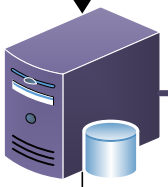
IANA

ASNs:
0-4294967295
IP Prefixes:
0.0.0.0/0



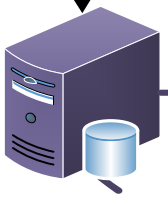
APNIC

ASNs:
64497-64510
65537-65550
IP Prefixes:
192.0.2.128/25
198.51.100.128/25
203.0.113.128/25



CNNIC

ASNs:
64498-64505
IP Prefixes:
192.0.2.128/26
198.51.100.128/26
203.0.113.128/26



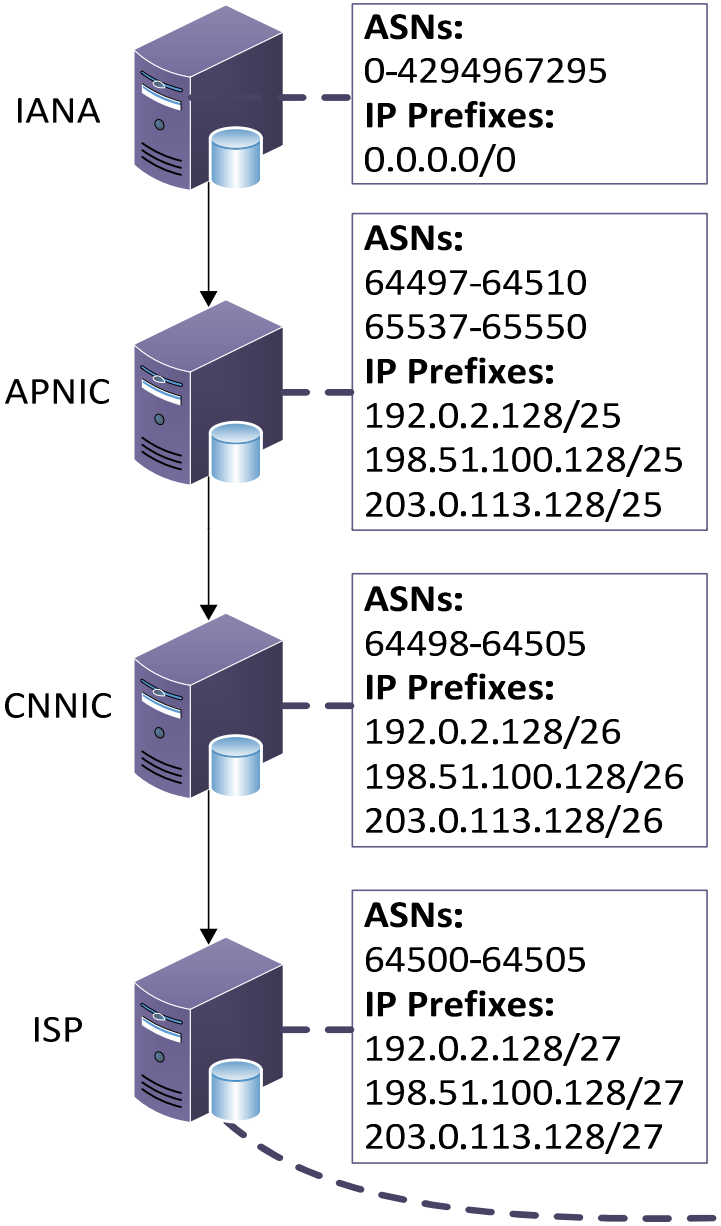
ISP

ASNs:
64500-64505
IP Prefixes:
192.0.2.128/27
198.51.100.128/27
203.0.113.128/27

```
test@~$cat ISPROA.csv
192.0.2.128/28  64500 Group1
198.51.100.128/28  64501 Group2
test@~$ rpkic -i ISP load_roa_requests ISPROA.csv
test@~$ rpkic -i ISP show_published_objects
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/duPylfF7Hv31rpOa4dVVCZnRkmk.crl
2017-07-19T10:34:04Z 594CB167AF4E81424EBEA7C1A5FD8DDE216D5C69
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/duPylfF7Hv31rpOa4dVVCZnRkmk.mft
2017-07-19T10:34:04Z 17C98CBFB179D60D9D0A6D52C2629B7A8DEA8A9C
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/M74Rq1am9m4YUairntkXTRAx6Wg.roa
2017-07-19T09:20:20Z 0CFD927D1522BF43FC52B748F274646387569222
64500 192.0.2.128/28
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/vulw_jMZBY7-KTN7nyhlpchBKZY.roa
2017-07-19T10:34:04Z 305866D0c4ee5e156ebeda811d3540bf0e094043
64501 198.51.100.128/28
```

ROA1:
64500->192.0.2.128/28
ROA2:
64501->198.51.100.128/28

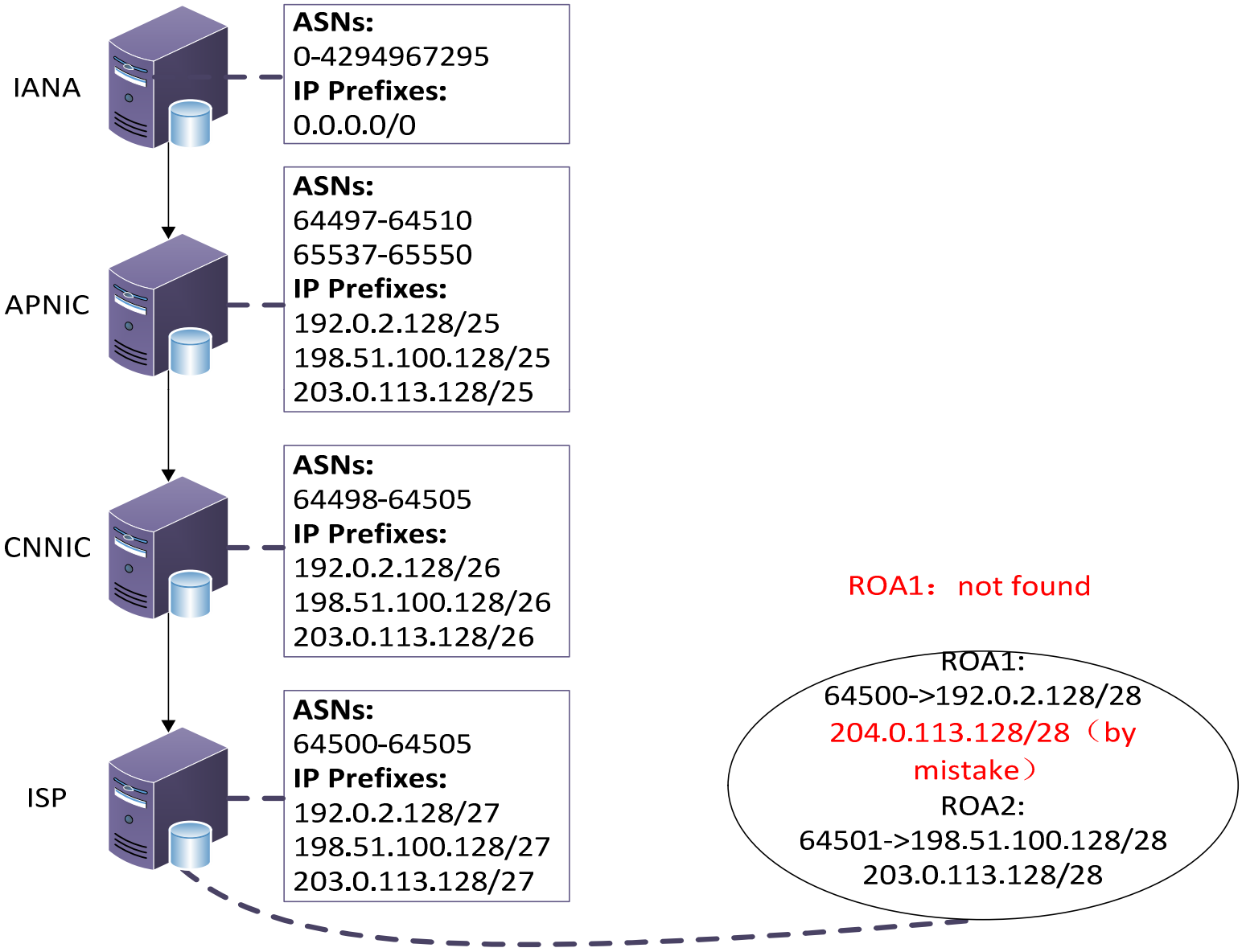
Experimental analysis




```
test@~$cat ISPROA.csv
192.0.2.128/28  64500 Group1
198.51.100.128/28  64501 Group2
203.0.113.128/28  64501 Group2
test@~$ rpkic -i ISP load_roa_requests ISPROA.csv
test@~$ rpkic -i ISP show_published_objects
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/duPylfF7Hv31rpOa4dVVCZnRkmk.crl
2017-07-19T10:38:03Z 2606EAA75AB60BE7785AE0CB0599D984AFD5BDB5
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/duPylfF7Hv31rpOa4dVVCZnRkmk.mft
2017-07-19T10:38:03Z 10F3F9249F0A6A636BF8143075693681B45A4BC2
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/M74Rq1am9m4YUairntkXTRAx6Wg.roa
2017-07-19T09:20:20Z 0CFD927D1522BF43FC52B748F274646387569222
64500 192.0.2.128/28
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/vO3whtjMpYxxyva4BxRqI2H8egA.roa
2017-07-19T10:38:03Z 4B85FDBABEC567A9DD8DA5745B34A201390F4530
64501 198.51.100.128/28,203.0.113.128/28
```

ROA1:
64500->192.0.2.128/28
ROA2:
64501->198.51.100.128/28
203.0.113.128/28（new add）

Experimental analysis



Experimental analysis

```
test@~$cat ISPROA.csv
192.0.2.128/28   64500 Group1
204.0.113.128/28 64500 Group1
198.51.100.128/28   64501 Group2
203.0.113.128/28   64501 Group2
test@~$ rpkic -i ISP load_roa_requests ISPROA.csv
test@~$ rpkic -i ISP show_published_objects
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/duPylfF7Hv31rpOa4dVVCZnRkmk.crl
2017-07-19T12:39:47Z 2DD037213237D72AF6CE95F8F37D1F08E8B49A37
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/duPylfF7Hv31rpOa4dVVCZnRkmk.mft
2017-07-19T12:39:47Z 735D9723B8C6D8214DA78117D27E529AA47E14B6
rsync://ubuntu/rpki/IANA/APNIC/CNNIC/ISP/vO3whtjMpYxxyva4BxRqI2H8eqA.roa
2017-07-19T10:38:03Z 4B85FDBABEC567A9DD8DA5745B34A201390F4530
64501 198.51.100.128/28,203.0.113.128/28
```

A legitimate ROA object was revoked because of ISP‘s misconfiguration. Obviously, this misconfiguration may lead to some serious consequences to RPKI (such as legitimate BGP routes are misclassified as “not found“)

Problem statement

- The misconfigurations of ROAs containing multiple IP address prefixes may lead to much more serious consequences than ROAs with fewer IP address prefixes.

- 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 convergence time of BGP routers and reduce their performance obviously

Suggestions and Considerations

- 1) The issuance of ROAs containing a large number of IP prefixes may lead to misconfigurations more easily than ROAs with fewer IP prefixes.
- it is recommended in the last paragraph of the section 4.2.5 of [I-D.ietf-sidr-rpki-validation-reconsidered] that opterators MAY issue separate ROAs for each IP address prefix, so that the loss of on IP address prefix from the VRS-IP of any certificate along the path to the trust anchor would not invalidate authorizations for other IP address prefixes.

Suggestions and Considerations

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

Comments?

Thank you