

RPKI ROAs for Unallocated and Unassigned AFRINIC Address Space

AFPUB-2019-GEN-006-DRAFT03

Frank Habicht (geier@geier.ne.tz)

Mark Elkins (mje@posix.co.za)

 @JordiPalet (jordi.palet@theipv6company.com)

Haitham El Nakhal (hytham@tra.gov.eg)

Summary of the problem

- Address space managed by AFRINIC which is either “Unallocated” or “Unassigned” is considered “Bogon address space”. As defined in RFC3871, A “Bogon” (plural: “bogons”) is a packet with an IP source address in an address block not yet allocated by IANA or the RIRs as well as all addresses reserved for private or special use by RFCs.
- The purpose of creating RPKI ROAs with Origin AS0 for AFRINIC’s unallocated and unassigned address space is to restrict the propagation of BGP announcements covering such bogon space. When AFRINIC issues a ROA with AS0 for unallocated address space under AFRINIC’s administration, BGP announcements covering this space will be marked as Invalid by networks doing RPKI based BGP Origin Validation using AFRINIC’s TAL

Addressing the problem

- This proposal instructs AFRINIC to create ROAs for all unallocated and unassigned address space under its control. This will enable networks performing RPKI-based BGP Origin Validation to easily reject all the bogon announcements covering resources managed by AFRINIC.
- Currently, in the absence of any ROA, these bogons are marked as NotFound. Since many operators have implemented ROV and either planning or already discarding Invalid, then all the AS0 ROAs which AFRINIC will create for unallocated address space will be discarded as well.
- The process for ROA validity periods and release of ROAs before assignment/allocation by AFRINIC is left for AFRINIC staff to define following usual internal procedures.

Proposed Text (1)

1 RPKI ROAs for Unallocated and Unassigned AFRINIC Address Space

AFRINIC will create ROAs with origin AS0 for all the unallocated and unassigned address space (IPv4 and IPv6) for which it is the current administrator.

Any resource holder can create AS0 (zero) ROAs for the resources they have under their account/administration.

An RPKI ROA is a positive attestation that a prefix holder has authorized an Autonomous System to originate a route for this prefix to the global BGP routing table. An RPKI ROA for the same prefixes with AS0 (zero) origin shows a negative intent from the resource holder to have the prefixes advertised in the global BGP routing table.

Only AFRINIC has the authority to create RPKI ROAs for address space not yet allocated or assigned to its members.

Proposed Text (2)

...

If AFRINIC wants to allocate address space to one of its members, the RPKI ROA or ROAs with origin AS0 will have to be revoked beforehand.

Address space can only be allocated once the ROA or ROAs with origin AS0 have been fully removed and are not visible in the repositories.

The AS0 ROAs could be under a distinct Trust Anchor Locator (TAL), so it becomes an opt-in service and provides separate measurements, at least in the initial deployment phases. This and other operational details are left to the discretion of AFRINIC.

AFRINIC should add reclaimed resources only at the end of the reclamation process.

What happened with v1 & v2?

- Unsubstantiated objections (regarding the government's using RPKI/ASO to censor networks), were accepted by the previous chairs, even if the authors and community experts refuted them, so it went back to discussion.
- Authors are unable to modify text based on an unsubstantiated objections, so we just added text based on the implementation experience in APNIC and to resolve clarifications requested by the v1 and v2 analysis impact.
- New analysis impact (v3) looks clear from our perspective and we addressed inputs from the previous discussions.

References

- APNIC has implemented it and is being used already:
 - <https://www.apnic.net/community/policy/proposals/prop-132>
 - https://www.youtube.com/watch?v=8_NnXDA6P24&t=34m57s
 - <https://conference.apnic.net/50/assets/files/APCS790/prop-132-Implementation.pdf>
 - <https://www.youtube.com/watch?v=UOBGjdTMN80&t=59m20s>
 - <https://conference.apnic.net/50/assets/files/APCS790/AS0-Implementation-report%20.pdf>
- An equivalent proposal is being implemented in LACNIC:
 - <https://politiclas.lacnic.net/politiclas/detail/id/LAC-2019-12?language=en>

RFC6483

Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)

(4. Disavowal of Routing Origination)

...

A ROA with a subject of AS 0 (AS 0 ROA) is an attestation by the holder of a prefix that the prefix described in the ROA, and any more specific prefix, should not be used in a routing context.

The route validation procedure, described in Section 2, will provide a "valid" outcome if any ROA matches the address prefix and origin AS, even if other valid ROAs would provide an "invalid" validation outcome if used in isolation. Consequently, an AS 0 ROA has a lower relative preference than any other ROA that has a routable AS as its subject. This allows a prefix holder to use an AS 0 ROA to declare a default condition that any route that is equal to or more specific than the prefix to be considered "invalid", while also allowing other concurrently issued ROAs to describe valid origination authorizations for more specific prefixes.

...

Responses to Impact Analysis

- All looks like 100% clear and nothing against this proposal.