Implementing RPKI-based origin validation ~~one~~ two ~~country~~ countries at a time.

The Ecuadorian and Costa Rican case studies

IETF 90 – TORONTO

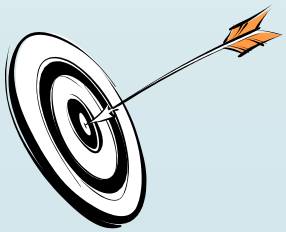
First presented in IETF 89 (SIDR) by Fabián Mejía

Sofia Silva

sofia AT lacnic.net

RPKI in NAP.EC: Project Goals

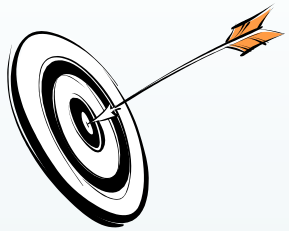
- **"Deploy RPKI-based BGP origin validation in NAP.EC's route servers"**
- Success threshold: 80% of the Ecuadorian prefixes (both IPv4 and IPv6) received by those routers should have a valid origin."
  - NAP.EC - GYE was chosen as the reference benchmark
    - NAP.EC - UIO sees prefixes from outside Ecuador making it harder to measure this 80%
- Wider goals:
  - Provide training in BGP and RPKI to the IXP's member community
  - Strengthen infrastructure in the region



Why and who?

- BGP origin validation based on RPKI is in its early stages of deployment. The participating organizations felt It is necessary to create success stories bringing value to all involved:
  - network operators
  - resource holders
  - Internet community
- Organizations involved: CISCO, LACNIC and AEPROVI.

ABSTRACT



I-D: draft-fmejia-opsec-origin-a-country-00.txt

- One possible deployment strategy for BGP origin validation based on the Resource Public Key Infrastructure (RPKI) is the construction of islands of trust. This document describes the authors' experience deploying and maintaining a BGP origin validation island of trust in Ecuador.

The authors want comments from this WG.

Roles

- **POLICING NETWORK:** NAP.EC (www.nap.ec). IXP in Ecuador (UIO and GYE). Mandatory multilateral routing policy. AEPROVI manages the NAP.EC infrastructure.

- **RESOURCE HOLDERS:** a number of holders, including organizations like ISP, content providers, universities, .ec domain and root servers administrators. Local and foreign organizations.

- **RPKI CAs AND REPOSITORY:** LACNIC's hosted RPKI service was used for this project.

- **TECHNICAL SUPPORT:** To involve trained people and train new ones is very important. Cisco and LACNIC staff collaborated.

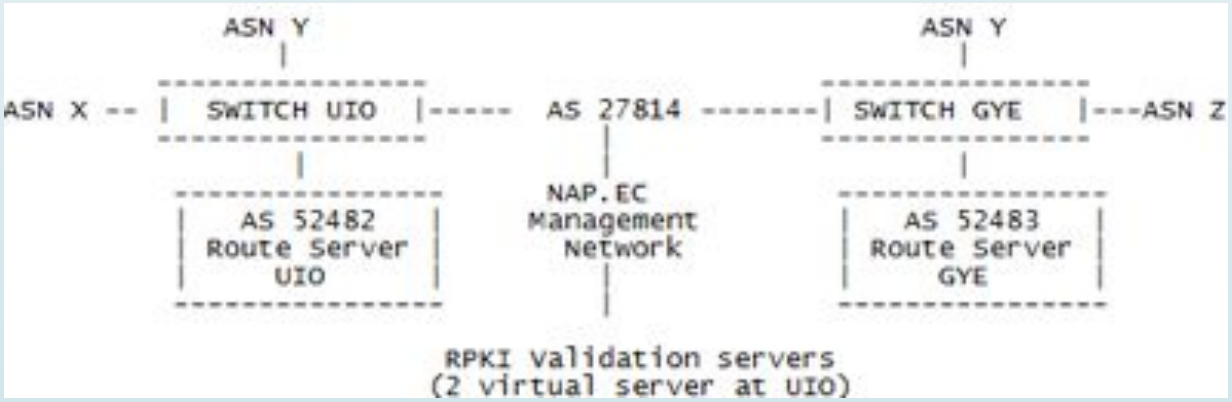
Planning

- Discussion points:
  1. RPKI-based origin validation support in the route-servers equipments
  2. How to deploy a RPKI cache into the Network
  3. How to populate the RPKI database with the correct and necessary information
  4. Action to take with NotFound and Invalid prefixes
- About 3: It was decided to organize an event with two objectives: training and RPKI object signing.
- Communication strategy should not be overlooked.

Deployment

RPKI Validation servers

- Two VMs running GNU Linux
- VMs are within management AS and access to Internet and both NAP.EC locations (UIO , GYE)
- Each VM runs 2 validating software: from RIPE and rpki.net project
- Different service ports



Deployment (II)

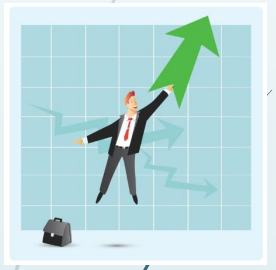
Origin validation policy

- No discard action taken at first
  - Prefix marking with a BGP community based on its RPKI origin validation state
- Afther 6 months it was decided to start dropping Invalid prefixes and setting a lower local preference for NotFound prefixes.

Training and RPKI signing event (aka ROA Party)

- Key planning activity: to create the list of participants and to make sure that at least one participant per network had the authentication credentials to create its RPKI signed objects.
- Target community: Ecuadorian organizations that had received IP resources from LACNIC until mid-2013.
- The attendance represented around 80% of the target prefixes.
- Two day training event including hands-on training plus turn-based assisted ROA creation

Outcome and post-event activities



- Ecuadorian prefixes with RPKI origin state as Valid:
  - Less 1% before the event.
  - Less than 20% at the start of the second day,
  - Around 80% at the end of the event.
  - Almost 100% a few days after the event, after to contact some non-attending organizations.
- After, some communication activities were performed.
- Overall, management has been simple and without major problems.

Lessons learned and best practices

- Implementation support needs to be verified in all target platforms
- The resource holders community need RPKI-based origin validation training
- Two days event is a better practice. The participants may not be confident about their skills at the end of the first day or may need further authorization
- Initial work to have the "right people" in the room is a key to success
- Operators are less conservative than originally though by the organizers
- When a new ISP wants to join NAP.EC, it receives information about RPKI-based origin validation and is invited to create its ROAs
- The event was a great opportunity to assemble the local community
- Post event communication needs to be discussed ahead of time.

IMPACT – LAC REGION

JULY 2013

RIR	Total	Valid	Invalid	Unknown	RPKI Adoption Rate
LACNIC	56294 (100%)	5561 (9.88%)	1184 (2.1%)	49549 (88.02%)	11.98%

OCTOBER 2013

RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
LACNIC	61506 (100%)	11336 (18.43%)	1109 (1.8%)	49061 (79.77%)	91.09%	20.23%

Fuente: http://rpki.surfnet.nl/perrir.html

IMPACT – COMPARATIVE

OCTOBER 2013

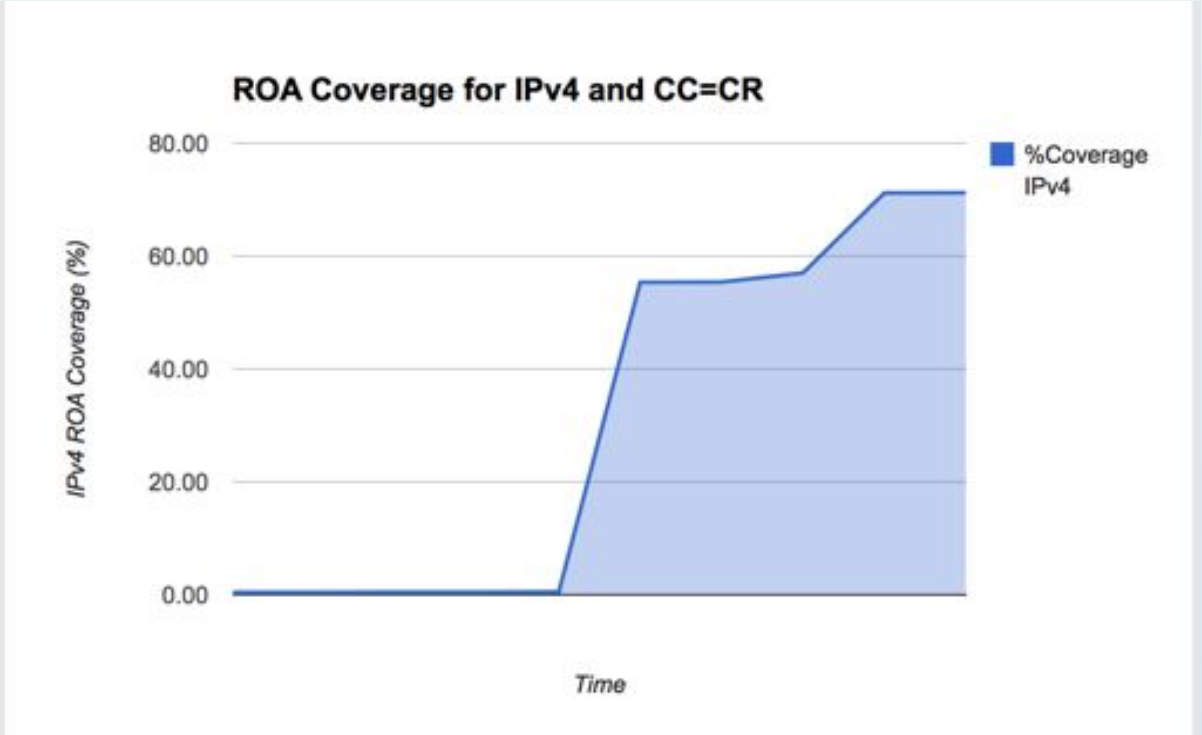
10 records per page Search:

RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
AFRINIC	11281 (100%)	41 (0.36%)	42 (0.37%)	11198 (99.26%)	49.4%	0.74%
APNIC	118423 (100%)	162 (0.14%)	236 (0.2%)	118025 (99.66%)	40.7%	0.34%
ARIN	186884 (100%)	649 (0.35%)	91 (0.05%)	186144 (99.6%)	87.7%	0.4%
LACNIC	61506 (100%)	11336 (18.43%)	1109 (1.8%)	49061 (79.77%)	91.09%	20.23%
RIPE NCC	131666 (100%)	7515 (5.71%)	1133 (0.86%)	123018 (93.43%)	86.9%	6.57%

Fuente: http://rpki.surfnet.nl/perrir.html

The Costa Rican Case

- A similar event was held in Costa Rica in June 2014
- Roles and structure of the event were very similar
  - http://labs.lacnic.net/site/rpki-en-el-ixp-costarica (in Spanish only yet, sorry)



Next Steps / Open Questions

- The authors believe that either informational or future BCP documents describing the experiences and operational lessons learned in these deployments are useful
- Questions:
  - Is it relevant / interesting work for OPSEC ?
  - ***Should it become a WG item ?***
- Next steps for the document:
  - Augment it with further experiences on similar deployments
    - We are already in talks with other actors in our region to conduct further similar activities
  - Augment it with considerations dealing with L2 vs L3 Internet Exchange Points

Thanks

Fabián Mejía

NAP.EC Administrator

fabian@aeprovi.org.ec