

Route Origin Authorization (ROA) using RPKI

Vivek Nigam

SANOG 26, Mumbai India

4 August 2015

APNIC

Issue Date: 31/12/2014

Revision: 1



Resource Public Key Infrastructure

What is RPKI?

- A robust security framework for verifying the association between **resource holders** and **their Internet resources**
- Uses x.509 certificates with RFC3779 extensions
- Collaborative effort by all RIRs to help secure Internet routing by validating routes

RFCs on RPKI

- **RFC 6810** – The Resource Public Key Infrastructure (RPKI) to Router Protocol (January 2013) – Standard
- **RFC 6480** – An Infrastructure to Support Secure Internet Routing (Feb 2012) - informational
- **RFC 6481** – A Profile for Resource Certificate Repository Structure (Feb 2012) - standard
- **RFC 6491** – RPKI Objects Issued by IANA
- **RFC 6493** – The RPKI Ghostbusters Record
- **RFC 6487** – A Profile for X.509 PKIX Resource Certificate

APNIC's involvement in RPKI

- Initial phase introduced by RIRs in 2009
- Initiative from APNIC aimed at
 - Improving the security of inter-domain routing
 - Augmenting the information published in the Whois database

Motivation

- Prevent route hijacking
 - Only the rightful custodian can originate the prefix announcement
 - ISPs filter prefixes they propagate
- Minimize common routing errors
 - Limits human errors
 - Prioritize routes with certificates

Real-life routing incidents

- **June 2015** - Telecom Malaysia causes large-scale routing issues due to route leak
- **April 2014** - Indosat leaked 32,000 routes
- **April 2010** - China Telecom advertisement causes 15% of Internet traffic to pass through Chinese servers
- **February 2008** - Pakistan Telecom announces 208.65.153.0/24 (YouTube prefix)

Route Origin Authorization (ROA)

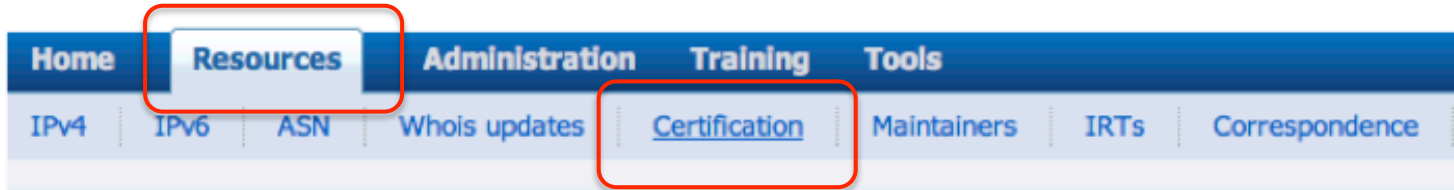
- What's contained in a ROA
 - The AS number you have authorized
 - The prefix that is being originated from it
 - The most specific prefix (maximum length) that the AS may announce

For example: “**AS64496** originates a route for the prefix **2001:DB8::/32** with a maximum prefix length of **/40**)”

Creating ROA in MyAPNIC

- What you need to have before creating a ROA
 - Must be an APNIC Member
 - Have access to MyAPNIC with 2 factor authentication
- Takes only 5 minutes to create, and 10 minutes to be visible to the public

Activate RPKI Engine



Select if you want to operate in the MyAPNIC RPKI portal or if you want to host your own certificate authority.

Home / Resources / RPKI

RPKI

Enable Resource Certification

Currently, you have not enabled resource certification for your registry.

- I want to operate in the MyAPNIC RPKI portal.
- I want to host my own certification authority and run an RPKI engine myself.

Next

Create your ROA (Using suggestions)

Home Resources Administration Events Contact Tools

IPv4 IPv6 ASN Whois updates Certification Maintainers IRTs

Home / Resources / RPKI

RPKI

1 ROA successfully marked for addition. Remember to commit you changes.

BGP Route Validity

1) Select your BGP route(s) from the list

Origin AS	Prefix
<input checked="" type="checkbox"/> 45192	2001:df0:a::/48
<input type="checkbox"/> 45192	203.176.189.0/24

Suggest ROAs

2) Click Suggest ROA button

Showing 1 to 2 of 2 entries

ROA Configuration

Origin ASN Prefix Max Length

Origin AS	Prefix	Max Length
45192	2001:df0:a::/48	48

Commit

3) Click Commit

Showing 1 to 1 of 1 entries

Certified Resources

- 61.45.248.0/23
- 61.45.251.0/24
- 61.45.253.0/24
- 203.176.189.0/24
- 2001:DF0:A::/48

Create your ROA (Manual)

ROA Configuration

1) Enter the Origin ASN you authorize to announce routes for your IP prefix

Origin ASN Prefix Max Length

4) Click Add

Certified Resources

- 61.45.248.0/23
- 61.45.251.0/24
- 61.45.253.0/24
- 203.176.189.0/24
- 2001:DF0:A::/48
- 2406:6400::/32

Origin AS	Prefix	Max Length	
45192	2001:df0:a::/48	48	
45192	203.176.189.0/24	24	

Showing 1 to 2 of 2 entries

2) Enter your IP prefix that is being announced

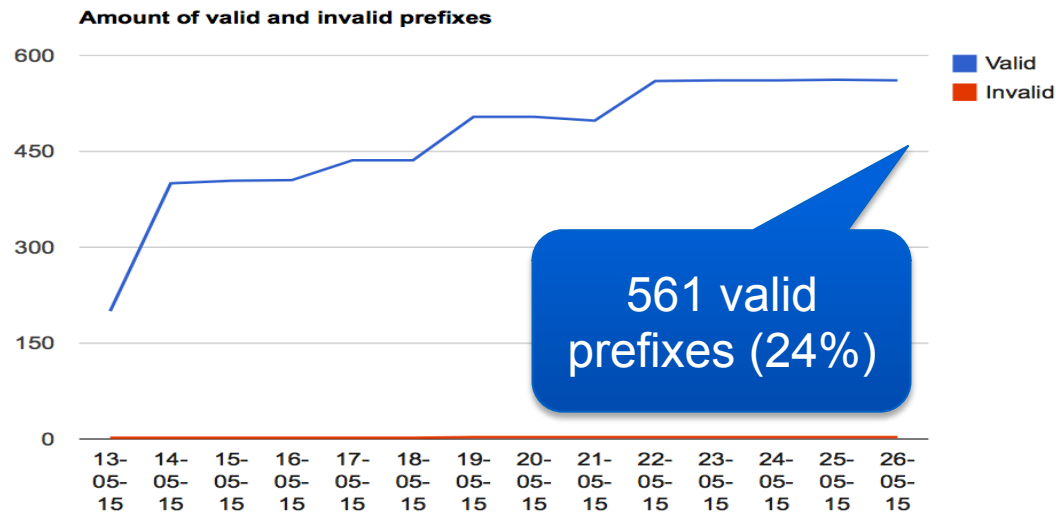
3) Enter the Max Length of prefix that you authorize for this ROA

Created your ROA, what's next?

- **Maintain your ROAs**
 - Changed BGP announcements
 - New delegations
 - Transferred resources
- **RPKI validator**
 - <https://trac.rpki.net/wiki/doc/RPKI>
 - Valid
 - Invalid
 - Unknown

Success Story

- May 2015: APNIC Outreach in Bangladesh
 - 13 organizations visited
 - Onsite support to create ROA objects



<http://rpkі.surfnet.nl/bd.html>

World Leaderboard

10 records per page

Search:

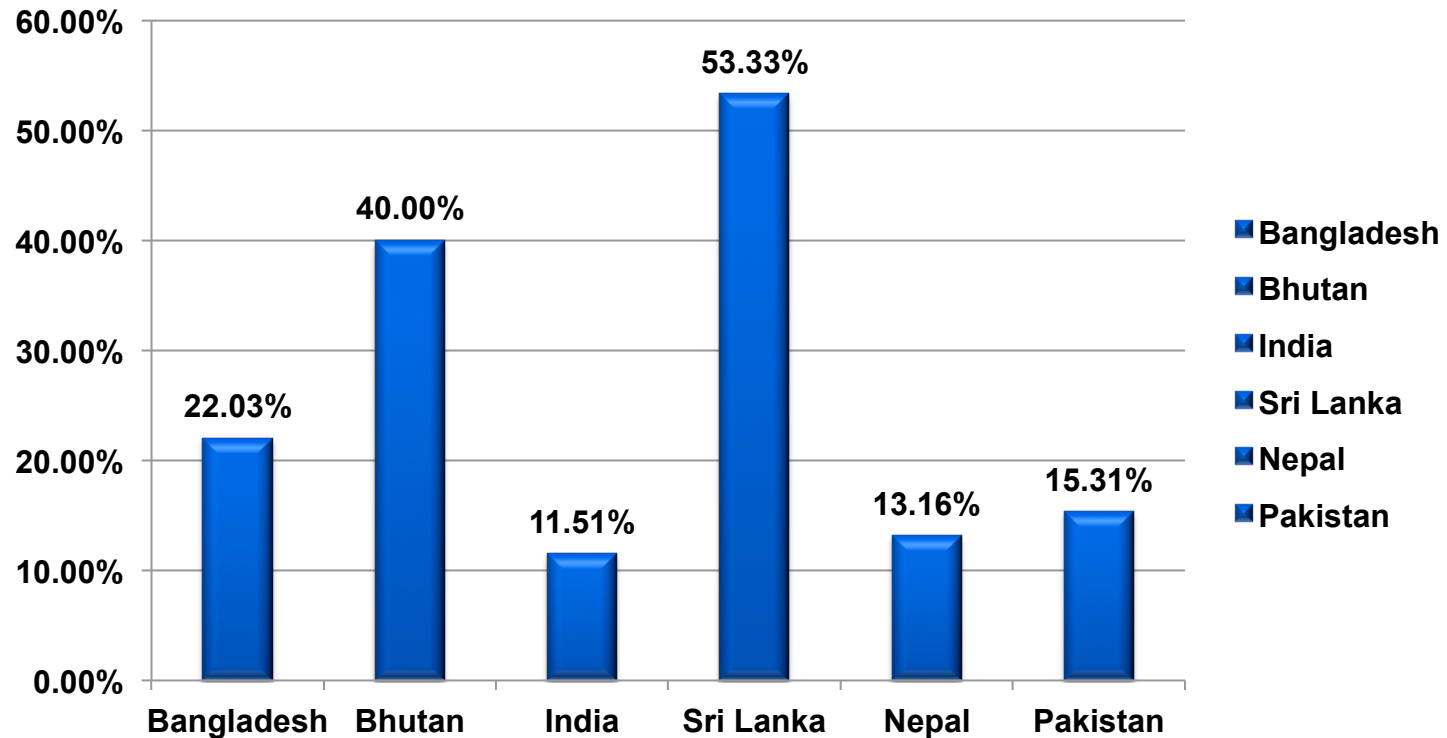
Country	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
BD	2336 (100%)	617 (26.41%)	5 (0.21%)	1714 (73.37%)	99.2%	26.63%
NL	5028 (100%)	656 (13.05%)	25 (0.5%)	4347 (86.46%)	96.33%	13.54%
FR	5834 (100%)	1154 (19.78%)	105 (1.8%)	4575 (78.42%)	91.66%	21.58%
US	174637 (100%)	1084 (0.62%)	331 (0.19%)	173222 (99.19%)	76.61%	0.81%

As of June 10, 2015

<http://rpki.surfnet.nl/country.html>

Story in South Asia

Resource Certification enabled members



As at 26/07/2015

RPKI Initiatives

**READY TO
ROA**



10 face-to-face and elearning RPKI training courses delivered

RPKI presentations to NOGs and conferences

Development of the 'Ready to ROA' Campaign – hands on sessions to help Members create ROAs

New shirts, stickers, web content to promote campaign

Ready to ROA launched in 2015

Have your say on MyAPNIC

- APNIC is gathering feedback to ensure MyAPNIC provides you with the best possible user experience and features.
 - <https://fluidsurveys.com/s/apnic/myapnicsurvey>
 - Lucky draw to win 1 of 20 wireless presenters



THANK YOU

APNIC

