The impact of an RPKI validator in Bangladesh and Lessons Learned

Md. Abdul Awal
NSRC
awal@nsrc.org

#ThaiNOG
May 14, 2021
Starting with some routing incidents...
• A Prefix is announced by both AS 134599 and AS 133957 (might be unintentional)
• Either AS cloud be closest to different geographic locations
• Legitimate traffic might get blackholed
• Issue informed to the IP owner.
• They removed one announcement
• Created ROA for valid ASN
• Valid announcement visible in the global routing table
• Client AS didn’t update APNIC membership
• Shouldn’t have valid prefix allocation with revoked membership
• Transit still announces client’s prefixes
• Prefixes marked as BOGON in global routing table
• The issue has been informed to the transit provider
• Then, they dropped it
• The announcement was removed from global table
• Later on, the AS got membership renewed and has its allocated prefixes back for use
103.204.210.0/24 was delegated by AS 64075 to AS 137842

AS 137842 announced the prefix

AS 64075 is also announcing its delegated prefixes as AS 137842 (AS Hijack)

It’s upstream accepting it and further announcing it globally

The issue has been informed to them and got fixed
• A /64 IPv6 prefix announced in global routing table
• Most specific announcement in global table is /48
• A /64 should never be in global routing table
• The issue was informed to the AS
• The announcement has been removed
Somebody is announcing non-routable prefixes in the global BGP table.

The announcement has been removed once the issue was informed to them.
• AS 136909 used to take transit via AS 24342 using static routing.
• AS 24342 announced prefixes of AS 136909 in global BGP table on their behalf.
• Later, AS 136909 stated doing BGP but AS 24342 still didn’t stop the announcement.
• AS 24342 has been informed to stop announcing client’s prefixes
• Client AS 136909 has signed their prefixes
• Issue resolved.
• AS 136901 got an allocation of /22.
• They announce part of its prefix (not the whole), e.g. /23 is announced but the other /23 is not.
• Opportunists can try to use the unannounced /23 for unauthorized activities.
• AS 137515 announced BCC’s prefix 103.48.17.0/24 to BDIX (Prefix hijack)

• Important government services became unavailable to the citizens

• Costs our time to fix.
What they reply about it? Funny but they really did

• We mistakenly announced the prefix
• We do not manually check our clients’ APNIC membership status
• The client is very trustworthy, so we never required to check their announcements
• We don’t do prefix or AS filtering for our clients
• Forgot to stop announcing the prefix after it’s delegated to another AS
How we ensure the routing hygiene manually? 

Nightmare...
RPKI is about 2 things: ROA and ROV

1. Signing prefixes
   a.k.a. creating ROAs

   - 2001:db8::/32
   - 192.0.2.0/24

   - RIR CA
   - RIR Resource DB
   - Member Login Authentication
   - ROA
   - AS 65000

   - Prefix: 2401:ED80::/32
   - Origin AS: AS63932
   - MSA: /32
   - ROA: Enabled
   - Whois: Enabled
   - Actions: Update whois

   - Route
     - 103.48.16.0/22
     - 2401:ED80::/32
     - 43.229.12.0/22
     - 43.229.15.0/24
     - Origin AS: AS63932
     - ROA status: 
     - Whois status: 

ThaiNOG 2021
RPKI is about 2 things: ROA and ROV

2. Validating ROAs
   a.k.a doing ROV

RPKI Repository  rsync/RRDP  RPKI Validator  RTR Protocol  BGP Router
Why Create ROA?

To ensure the authenticity of your IP resources and help others verify it if requires.

So that your IP resources are not knowingly or unknowingly used or abused by anyone.
Why Deploy ROV?

- To build and maintain a secure and trustworthy global routing infrastructure
- To validate BGP routes and identify the authorized originator of the prefix
RPKI Validation in NDC and subsequent impact
RPKI Validation at National Data Center

• NDC declared to drop invalids since Dec 1, 2019
• Bangladesh has more than 800 active ASN
• BD ROA stats in Sep 2019:
  • Valid – 29%
  • Unknown – 69%
  • Invalid – 2%
• Need to find out ASNs who are getting impact
  • BD ASNs are easy to reach for obvious reason
  • How about the global ASNs?
Awareness Before the ROV

Subject: NDC starts RPKI Validation on Dec 1  
Date: Thu, 7 Nov 2019 00:44:32 +0000  
From: Md. Abdul Awal <awal.ece@gmail.com>  
To: nog <nog@bdnog.org>

Dear Colleagues,

National Data Center (NDC) at Bangladesh Computer Council (BCC) starts RPKI ROA validation on December 1, 2019.

Read more here:  
https://www.cirt.gov.bd/%e0%a6%9c%e0%a6%be%e0%a6%90%e0%a7%81%e6%b9%e0%a6%87%e0%a6%95%e0%a6%be%e0%a6%b0%

NDC team tried to reach ASNs who have INVALID ROAs and helped many of them to fix it. However, there are still about 2% invalid prefixes in Bangladesh. Please be informed that the INVALID prefixes would not be able to access any content hosted at NDC after Nov 30.

Please spend some time to check the ROA for your prefixes. Correct any invalid ROAs immediately from your MyAPNIC portal. Also, if you didn’t create ROA for your prefixes yet, please do so asap.

Best regards,  
Awal  
ThaiNOG 2021
Awareness Before the ROV

• We helped others to create and/or fix their ROAs
  • LEAs, Police, Special forces
  • Govt. Organizations
  • IXPs
  • Banks and Financial Organizations
  • Transit providers
  • ISPs
  • Data Centers
The impact of awareness campaign

<table>
<thead>
<tr>
<th>Prefix</th>
<th>123.49.0.0/18</th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>123.49.14.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>123.49.16.0/20</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>123.49.29.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>123.49.30.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>123.49.31.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>123.49.47.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>180.211.128.0/17</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>180.211.201.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>180.211.214.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>180.211.215.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>203.112.192.0/19</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>203.112.194.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>209.58.24.0/24</td>
<td>✓</td>
</tr>
<tr>
<td>Prefix</td>
<td>123.49.0.0/18</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>123.49.14.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>123.49.16.0/20</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>123.49.29.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>123.49.30.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>123.49.31.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>123.49.47.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>180.211.128.0/17</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>180.211.201.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>180.211.214.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>180.211.215.0/24</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>203.112.192.0/19</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>203.112.194.0/24</td>
<td>✓</td>
</tr>
</tbody>
</table>

Source: https://bgp.he.net
ThaiNOG 2021
The impact of awareness campaign

<table>
<thead>
<tr>
<th>Prefix</th>
<th>AS Info</th>
<th>Graph v4</th>
<th>Prefixes v4</th>
<th>Peers v4</th>
</tr>
</thead>
<tbody>
<tr>
<td>43.255.20.0/22</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43.255.20.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43.255.21.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43.255.22.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.239.4.0/22</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.239.4.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.239.5.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.239.6.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.239.7.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prefix</th>
<th>AS Info</th>
<th>Graph v4</th>
<th>Prefixes v4</th>
<th>Peers v4</th>
</tr>
</thead>
<tbody>
<tr>
<td>43.255.20.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43.255.21.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43.255.22.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.239.4.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.239.5.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.239.6.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.239.7.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The impact of awareness campaign

Routing completeness (RPKI)

Sep 2019

Oct 2019

Nov 2019

Source: https://observatory.manrs.org
And, finally NDC drops invalids since Dec 1, 2019
The impact of awareness campaign

![Comparison of routing completeness (RPKI) between Dec 2019 and Jan 2020](image)

**Dec 2019**

- Total: 100%
  - Valid: 70%
  - Unknown: 29%
  - Invalid: 2%

**Jan 2020**

- Total: 100%
  - Valid: 72%
  - Unknown: 27%
  - Invalid: 1%

Source: https://observatory.manrs.org
The impact of awareness campaign

Source: https://stat.ripe.net/BD#tabId=routing

ThaiNOG 2021
The impact of awareness campaign

Source: https://stat.ripe.net/BD#tabId=routing
RPKI ROA Adoption in BD

Source: https://observatory.manrs.org

ThaiNOG 2021
Considerations about ROA and ROV
Creating ROA

- Not a good idea to create ROAs up to /24 if not announced in BGP
- Better to create ROAs for specific prefixes that are announced in BGP
Creating ROA

You may sign same prefix with multiple ASNs but do if you really really have to
Doing ROV

Validation without dropping RPKI Invalids

VS

Validation with dropping RPKI Invalids
ROA for Small ISPs and Enterprises

- Have own Internet resources?
  - Creating ROA is straightforward using RIR’s resource management portal
- Got assignment for LIR?
  - Have public ASN?
    - Ask the LIR to create ROA with your ASN and verify
  - Don’t have public ASN?
    - Ask the LIR to create ROA for the assigned prefix and verify
ROV for Small ISPs and Enterprises

• Have BGP with transits and peers?
  • Receive full routes from neighbors?
    • Implementing ROV using validator cache is straightforward
  • Receive partial routes with default from neighbors?
    • Ask transits to do ROV for you
    • Implement ROV using validator cache to validate peer and IX routes
  • Receive only the default route
    • ROV wouldn’t fit, however, you may ask transits to do ROV on their network 😊

• Have static routing with transits?
  • ROV wouldn’t fit, however, you may ask transits to do ROV on their network
Still thinking why we need ROA and ROV?

- Check the issues discussed in first couple slides
- Reduce the opportunity of routing incidents, prefix hijacks, route leaks, DDoS, outages
- You wouldn’t want to be a target of those incidents
- Help improve global routing infrastructure security
- Help each other to maintain routing hygiene
- We are engineers working hard to make Internet better, remember?
We all can help improve global routing security

• Create/fix ROAs for your prefixes
• If you are a transit provider, ask you clients to do the same
• If you’re receiving BGP full route, implement ROV
• Share this among other colleagues in the community
• Help others fix their ROAs
Let’s check your own ASN

- Go to https://bgp.he.net, search for your AS number and check v4 and v6 prefixes

Or,

- Use whois on unix terminal:

  whois -h whois.bgpmon.net " --roa ASN Prefix"

- If you find issues with ROA, please fix it

References

1. https://learn.nsrc.org/bgp/MANRS4_RPKI_and_ROA
3. https://www.manrs.org/manrs
5. https://www.apnic.net/get-ip/faqs/rpki/
Questions?