Secure Inter-domain Routing with RPKI

Srinivas (Sunny) Chendi
VNIX-NOG 2018, Da Nang
sunny@apnic.net

Xin chào và chào buổi sáng
I don't care what you think. Peanuts are important!
What is the fundamental Problem?
An underlying problem in routing is lack of certainty

• BGP is a giant ‘rumor’ system:
  – What I hear I pass on.
  – What I hear, I reflect on, deciding to route.
  – Has two primary properties to be tested: **Origination** and **Path**

• Why do I believe what I hear?
An underlying problem in routing is lack of certainty

- **Origination** binds a prefix to a specific Autonomous System (AS) number
  - The Origin-AS (of the prefix) is chosen by the prefix holder
  - **Bad actors can claim to originate. How do we limit this risk?**

- **Path** binds an Origin-AS to the set of intermediate Autonomous Systems forwarding between themselves (transit) towards the Origin-AS
  - The inter-AS relationships are chosen by the operators of the AS
  - Therefore the AS-PATH elements over any given origin-AS/Prefix pair is a reflection of the specific AS operator(s) along the path
  - **Bad actors can intermediate themselves into path. How do we limit this risk?**
Telekom Malaysia

• On June 12, 2015, Telekom Malaysia (AS4788) tweets this then breaks the Internet

• It announced 179,000 prefixes to Level 3 (AS3549)

http://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/
Indonesia Hijacks

• In April 2014, Indosat (AS4761) leaked over 320,000* routes within a 2-hour period
• Disrupted Akamai
• Self-inflicted DDoS attack

http://research.dyn.com/2015/06/global-collateral-damage-of-tmnet-leak/
YouTube Incident

• Before: YouTube announces 208.65.152.0/22 from AS36561
• 24 Feb 2008:
  – Pakistan Telecom asked to block YouTube (by Telecommunications Ministry)
  – PT (AS17557) mistakenly announced 208.65.153.0/24
  – The upstream PCCW (AS3491) propagated this worldwide
  – Route: 208.65.153.0/24 {…} 3491 17557
  – YouTube traffic redirected to PT (longest match rule)
• Google announced 208.65.153.0/24
  – Traffic goes to either AS36561 or AS17557 based on shortest path

Ref: Youtube Hijacking: A RIPE NCC Case Study
Misdirection / Hijacking Incidents

• YouTube Incident
  – Occurred 24 Feb 2008 (for about 2 hours)
  – Pakistan Telecom announced YT block

• Google (AS15169) services downed
  – Occurred 5 Nov 2012 (for 30 minutes)
  – Moratel Indonesia (AS23947)
How Do We Collaboratively Solve This Problem?
How we address this…

A network should only originate his own prefix

*How do we verify & avoid false advertisement?*

A provider should filter prefixes they propagate from customers

- Transitive trust; BGP is a trust-based system
- Check the legitimacy of address (LoA)
- Passive Countermeasure

Strict filter on Interconnection

- BGP router can filter in UPDATE Messages
- Useful filtering can be done by upstream provider

Automate Filter Maintenance

- Use the Route Object
What is RPKI?
What is RPKI?

• A robust security framework for verifying the association between resource holder and Internet resource

• Helps to secure Internet routing by validating routes
X.509 Certificate with 3779 Extension

- Resource certificates are based on the X.509 v3 certificate format defined in RFC 5280
- Extended by RFC 3779 – binds a list of resources (IP, ASN) to the subject of the certificate
- SIA – Subject Information Access; contains a URI that references the directory
RPKI Building Blocks

1. PKI and Trust anchors
2. Route Origin Authorizations (ROA)
3. RPKI Validators
What does it solve?

• Prevents **route hijacking**
  – A prefix originated by an AS without authorization due to malicious intent

• Prevents **mis-origination**
  – A prefix that is mistakenly originated by an AS which does not own it
  – Also route leakage
  – due to configuration mistake or fat finger
How does it work?

Is this AS number (ASN) authorized to announce this IP address range?
RPKI Origin Validation

<table>
<thead>
<tr>
<th>Prefix</th>
<th>AS Numbers</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2406:6400::/48</td>
<td>65551 65550 65549</td>
<td>VALID</td>
</tr>
<tr>
<td>2406:6400::/48</td>
<td>65551 65550 65548</td>
<td>INVALID</td>
</tr>
</tbody>
</table>

I have 2406:6400::/48

I have 2406:6400::/48
RPKI Path Validation

2406:6400::/48  65551 65550 65549

Check and verify the complete path (BGPSEC)
Main Components

• Certificate Authority (CA)
  – Internet registries (RIR, NIR, LIR)
  – Issues certificates to members (delegates with resources)
  – Allows address holders to use the CA system to issue ROAs for their prefixes

• Relying Party (RP)
  – Software that gathers data from the CA
Issuing Party

- Internet Registries (RIR, NIR, Large LIRs)
- Acts as a Certificate Authority and issues certificates to members with resources
- Often provides a web interface to issue ROAs for customer prefixes
- Publishes the ROA records into a repository
Relying Party

Software which gathers data from CAs
Also called RP cache or validator
Trust Anchors

Resource Allocation Hierarchy

AFRINIC  RIPE NCC  APNIC  APNIC  LACNIC

Issued Certificates match allocation actions

IANA

Trust Anchor Certificate

NIR  NIR

ISP  ISP  ISP  ISP  ISP
Route Origin Authorization (ROA)

• A signed digital object that contains a list of address prefixes and one AS number

• It is an authority created by a prefix holder to authorize an AS Number to originate one or more specific route advertisements

<table>
<thead>
<tr>
<th>Prefix originated</th>
<th>203.176.189.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum prefix length</td>
<td>/24</td>
</tr>
<tr>
<td>Origin ASN</td>
<td>AS17821</td>
</tr>
</tbody>
</table>

• ROA is valid if a valid certificate which signs it has the prefix in its RFC 3779 extension
RPKI Validation

- RPKI-capable routers can fetch the validated ROA dataset from a validated cache

<table>
<thead>
<tr>
<th>status</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VALID</td>
<td>Indicates that the prefix and ASN pair has been found in the database</td>
</tr>
<tr>
<td>INVALID</td>
<td>Indicates that the prefix is found, but</td>
</tr>
<tr>
<td></td>
<td>• ASN received did not match, or</td>
</tr>
<tr>
<td></td>
<td>• the prefix length is longer than the maximum length</td>
</tr>
<tr>
<td>NOT FOUND / UNKNOWN</td>
<td>Indicates that the prefix does not match any in the database</td>
</tr>
</tbody>
</table>
RPKI Deployment and Operations
RPKI Deployment and Operations

• RPKI Deployment
  - APNIC-hosted
  - Self-hosted

• RPKI Operations
  - Router configuration for origin validation
  - Route states and preference adjustment
RPKI Deployment: APNIC-hosted

• Enable RPKI in MyAPNIC
  - Set up two-factor authentication
  - Ensure permissions are set correctly

• Register routes using route management tool
  - Covers both RPKI and Whois (IRR)
To do

- **Invalid maintainers password**
  One or more of your maintainers has an invalid password. Click here to update them.

- **Pending registrations**
  There are pending user registrations for this account. Click here to process them.

- **Set up RPKI**
  Click here to set up RPKI.

Quick links

- Whois Updates
- Manage Account Contacts
- Add Reverse Delegations
- Annual Fee Calculator

Live chat

APNIC Live Chat
Offline
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
RPKI

Enable Hosted Resource Certification

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

Terms and Conditions of APNIC Certification Authority

Introduction

APNIC publishes all Certificates, Certificate Revocation Lists (CRLs), and RPKI-signed objects in the Certification Repository ("Repository"). The Repository is available to anyone under these Terms and Conditions.

Article 1 - Definitions

In the Terms and Conditions, unless the context requires otherwise, the following terms have the meanings assigned to them below:
Article 5 - Miscellaneous

APNIC's intellectual property (agreements, documents, software, databases, website, etc.) may only be used, reproduced and made available to third parties upon prior written authorisation from APNIC.

If any provision contained in the Terms and Conditions is held to be invalid by a court of law, this shall not in any way affect the validity of the remaining provisions.

Article 6 - Governing Law

These Terms and Conditions shall be exclusively governed by the laws of Queensland, Australia. The competent court in Queensland, Australia has exclusive jurisdiction with regard to disputes arising from these Terms and Conditions.
MyAPNIC

Home / Resources / RPKI

RPKI

Your RPKI engine has been activated. To enable ROA for routes, please click here to go to the Routes page.

Certified Resources

The following resources are included in your current resource certificates

203.147.108.0/23
203.176.189.0/24
2001:DF2:E500::/48
2401:E640::/32
Register your routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database with any AS number you have authorized. RPKI ROAs will also be created at the same time, if the ROA option is enabled (changes to RPKI may take around ten minutes to propagate so the ROA status will not be updated until then).

Create route   Delete selected

Show 10 entries  Search:

Route Origin AS ROA status Whois status Actions

No data available in table

Showing 0 to 0 of 0 entries  Previous  Next

© APNIC | Feedback | About MyAPNIC | Need help?
Create route

Prefix: Route’s prefix. E.g. 203.10.0.0/20

Origin AS: Route’s origin. E.g. AS123

Most specific announcement: Route’s most specific announcement. E.g. /22

ROA: Enabled

Whois: Enabled

- Define Whois route attributes

Options: Notify additional contacts

Cancel  Next
Create route

Prefix: 203.147.108.0/23
Origin AS: AS123456
Most specific announcement:

- ROA: Enabled
- Whois: Enabled
- Define Whois route attributes: Unchecked
- Notify additional contacts: Unchecked

[Cancel] [Next]
<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROA</td>
<td>Enabled</td>
</tr>
<tr>
<td>Whois</td>
<td>Enabled</td>
</tr>
<tr>
<td>Prefix</td>
<td>203.147.108.0/23</td>
</tr>
<tr>
<td>Origin AS</td>
<td>AS123456</td>
</tr>
<tr>
<td>Most specific announcement</td>
<td>/23</td>
</tr>
</tbody>
</table>
Routes

Register your routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database with any AS number you have authorized. RPKI ROAs will also be created at the same time, if the ROA option is enabled (Changes to RPKI may take around ten minutes to propagate so the ROA status will not be updated until then).

Create route  Delete selected

Show 10 entries

<table>
<thead>
<tr>
<th>Route</th>
<th>Origin AS</th>
<th>ROA status</th>
<th>Whois status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>203.147.108.0/23</td>
<td>AS123456</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>

Showing 1 to 1 of 1 entries

© APNIC | Feedback | About MyAPNIC | Need help?
Where Are We In Deployment Of RPKI?
Address holding and participation in RPKI, APNIC resources (from Repository products)
Prefix coverage in ROA against total deployed, APNIC resources

% of INR covered

IPv4% covered by ROA
IPv6% covered by ROA
“its not looking compelling”

- There is no strong visible trend in the last year suggestive of a surge in Asia-Pacific RPKI participation
  - There is increase, but its incremental, not exponential (I think)
  - Even if it was exponential, its very very early-life

- Rate of growth is below the rate of growth in participation overall
  - We give out more address space, to more people, than join to publish ROA

- Changes in ROA state are ‘lumpy’ correlating with specific ISPs changing their RPKI signing state.
  - Low levels of participation mean large swings visible

- Conclusion: we are still in early adoption phase of the life cycle of RPKI in the Asia-Pacific region
  - Key drivers are **training**, and directed engagement or **outreach**
### RP by ASN, by Economy

<table>
<thead>
<tr>
<th>Economy</th>
<th>Economy</th>
<th>Economy</th>
<th>Economy</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>US</td>
<td>23</td>
<td>DE</td>
<td>14</td>
</tr>
<tr>
<td>11</td>
<td>JP</td>
<td>9</td>
<td>FR</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>GB</td>
<td>5</td>
<td>CH</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>UA</td>
<td>2</td>
<td>TH</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>NZ</td>
<td>2</td>
<td>NO</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>IT</td>
<td>2</td>
<td>HU</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>AU</td>
<td>2</td>
<td>AT</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>UY</td>
<td>1</td>
<td>TW</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>RS</td>
<td>1</td>
<td>RO</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>MY</td>
<td>1</td>
<td>MV</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>LV</td>
<td>1</td>
<td>KR</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>CY</td>
<td>1</td>
<td>CR</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>BE</td>
<td>1</td>
<td>AR</td>
<td>1</td>
</tr>
</tbody>
</table>
## Participation by Economy in RPKI (ROA) APNIC resources. March 2017

<table>
<thead>
<tr>
<th>Economy</th>
<th>Active</th>
<th>Have Roa</th>
<th>%</th>
<th>Economy</th>
<th>Active</th>
<th>Have Roa</th>
<th>%</th>
<th>Economy</th>
<th>Active</th>
<th>Have Roa</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>AP</td>
<td>154</td>
<td>10</td>
<td>6.5</td>
<td>AU</td>
<td>2715</td>
<td>52</td>
<td>1.9</td>
</tr>
<tr>
<td>BD</td>
<td>394</td>
<td>56</td>
<td>14.2</td>
<td>BT</td>
<td>7</td>
<td>2</td>
<td>28.6</td>
<td>CN</td>
<td>2853</td>
<td>4</td>
<td>0.1</td>
</tr>
<tr>
<td>FJ</td>
<td>13</td>
<td>3</td>
<td>23.1</td>
<td>GU</td>
<td>9</td>
<td>1</td>
<td>11.1</td>
<td>HK</td>
<td>822</td>
<td>15</td>
<td>1.8</td>
</tr>
<tr>
<td>ID</td>
<td>1142</td>
<td>5</td>
<td>0.4</td>
<td>IN</td>
<td>2655</td>
<td>19</td>
<td>0.7</td>
<td>JP</td>
<td>1148</td>
<td>8</td>
<td>0.7</td>
</tr>
<tr>
<td>KH</td>
<td>68</td>
<td>9</td>
<td>13.2</td>
<td>KI</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>KR</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LA</td>
<td>16</td>
<td>2</td>
<td>12.5</td>
<td>LK</td>
<td>17</td>
<td>9</td>
<td>52.9</td>
<td>MM</td>
<td>45</td>
<td>10</td>
<td>22.2</td>
</tr>
<tr>
<td>MN</td>
<td>42</td>
<td>3</td>
<td>7.1</td>
<td>MV</td>
<td>10</td>
<td>2</td>
<td>20</td>
<td>MY</td>
<td>227</td>
<td>10</td>
<td>4.4</td>
</tr>
<tr>
<td>NC</td>
<td>10</td>
<td>2</td>
<td>20</td>
<td>NP</td>
<td>47</td>
<td>13</td>
<td>27.7</td>
<td>NZ</td>
<td>935</td>
<td>30</td>
<td>3.2</td>
</tr>
<tr>
<td>PG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>PF</td>
<td>5</td>
<td>2</td>
<td>40</td>
<td>PH</td>
<td>207</td>
<td>16</td>
<td>7.7</td>
</tr>
<tr>
<td>PK</td>
<td>138</td>
<td>15</td>
<td>10.9</td>
<td>SG</td>
<td>368</td>
<td>27</td>
<td>7.3</td>
<td>TH</td>
<td>194</td>
<td>12</td>
<td>6.2</td>
</tr>
<tr>
<td>TO</td>
<td>4</td>
<td>1</td>
<td>25</td>
<td>TW</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>VU</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WS</td>
<td>5</td>
<td>3</td>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Participation by Economy in RPKI (ROA)

APNIC resources. August 2018

<table>
<thead>
<tr>
<th>Economy</th>
<th>Active</th>
<th>Have Roa</th>
<th>%</th>
<th>Economy</th>
<th>Active</th>
<th>Have Roa</th>
<th>%</th>
<th>Economy</th>
<th>Active</th>
<th>Have Roa</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF</td>
<td>54</td>
<td>5</td>
<td>9.3</td>
<td>AP</td>
<td>150</td>
<td>14</td>
<td>9.3</td>
<td>AU</td>
<td>2878</td>
<td>92</td>
<td>3.2</td>
</tr>
<tr>
<td>BD</td>
<td>575</td>
<td>112</td>
<td>19.5</td>
<td>BT</td>
<td>9</td>
<td>3</td>
<td>33.3</td>
<td>CN</td>
<td>3250</td>
<td>33</td>
<td>1</td>
</tr>
<tr>
<td>FJ</td>
<td>16</td>
<td>3</td>
<td>18.8</td>
<td>GU</td>
<td>10</td>
<td>1</td>
<td>10</td>
<td>HK</td>
<td>897</td>
<td>33</td>
<td>3.7</td>
</tr>
<tr>
<td>ID</td>
<td>1467</td>
<td>11</td>
<td>0.7</td>
<td>IN</td>
<td>3088</td>
<td>43</td>
<td>1.4</td>
<td>JP</td>
<td>1178</td>
<td>36</td>
<td>3.1</td>
</tr>
<tr>
<td>KH</td>
<td>86</td>
<td>15</td>
<td>17.4</td>
<td>KI</td>
<td>2</td>
<td>1</td>
<td>50</td>
<td>KR</td>
<td>195</td>
<td>1</td>
<td>0.5</td>
</tr>
<tr>
<td>LA</td>
<td>20</td>
<td>7</td>
<td>35</td>
<td>LK</td>
<td>17</td>
<td>11</td>
<td>64.7</td>
<td>MM</td>
<td>62</td>
<td>14</td>
<td>22.6</td>
</tr>
<tr>
<td>MN</td>
<td>45</td>
<td>16</td>
<td>35.6</td>
<td>MV</td>
<td>13</td>
<td>2</td>
<td>15.4</td>
<td>MY</td>
<td>258</td>
<td>16</td>
<td>6.2</td>
</tr>
<tr>
<td>NC</td>
<td>11</td>
<td>4</td>
<td>36.4</td>
<td>NP</td>
<td>73</td>
<td>23</td>
<td>31.5</td>
<td>NZ</td>
<td>964</td>
<td>35</td>
<td>3.6</td>
</tr>
<tr>
<td>PK</td>
<td>160</td>
<td>24</td>
<td>15</td>
<td>PG</td>
<td>24</td>
<td>3</td>
<td>12.5</td>
<td>PH</td>
<td>230</td>
<td>23</td>
<td>10</td>
</tr>
<tr>
<td>TO</td>
<td>4</td>
<td>1</td>
<td>25</td>
<td>SG</td>
<td>401</td>
<td>36</td>
<td>9</td>
<td>TH</td>
<td>207</td>
<td>18</td>
<td>8.7</td>
</tr>
<tr>
<td>WS</td>
<td>5</td>
<td>4</td>
<td>80</td>
<td>TW</td>
<td>223</td>
<td>7</td>
<td>3.1</td>
<td>VU</td>
<td>11</td>
<td>1</td>
<td>9.1</td>
</tr>
</tbody>
</table>
Regional Participation is rising

• Overall, there is an increase in participation both absolutely and as a percentage in most leading economies
• There is significant headroom for improvement
• Launch of service from CNNIC, IDNIC, TWNIC should permit rapid increase
  – JPNIC has been in service for the past two years with significant deployment
  – IRINN (and IDNIC at present) operate on behalf of their members inside APNIC services (MyAPNIC portal, for NIR)
• Some indications that participation is more a function of outreach than anything else
  – When we do RPKI training, engagement from that economy rises.
Conclusions

• RPKI is our best mechanism for identifying the responsibility to control and route Internet Number Resources worldwide
  – It respects the RFC2050 delegation hierarchy
  – For Vietnamese INR holders, it will respect the authority of VNNIC in the management of resources which vest through VNNIC
  – Local Trust Anchors can be considered to avoid loss of authority from outside actions

• Although secure BGP is a work in progress and visible validation is low, there is still benefit to participation by INR holders
  – It sets a mark in public of your intent, and authority
  – Future models may provide new ways to use RPKI products in provisioning

• Vietnam is well placed to take a significant stance in secure routing.
  – National coordinating bodies exist, who understand the problems
  – The integrity of routing inside and outside Vietnam is understood to be critically important
Look ahead!
Cám ơn bạn

blog.apnic.net

apnic.net/social
Additional Information
RPKI Operations: Router Configuration

- Set up an RPKI validator
- Set up communication with the RPKI Validator
  - router bgp 10
  - bgp bestpath prefix-validate disable
  - bgp rpki server tcp 192.168.56.1 port 8282 refresh 300
- Verify the connection to the RPKI validator
  - show ip bgp rpki table
- Allow invalid routes to be used when no others are available
  - bgp bestpath prefix-validate allow-invalids
- Re-enable validation
  - no bgp bestpath prefix-validate disable
RPKI Operations: Router Configuration

```
test-rtr> show ip bgp rpkj table
1030 BGP sovc network entries using 90640 bytes of memory
1113 BGP sovc record entries using 22260 bytes of memory

<table>
<thead>
<tr>
<th>Network</th>
<th>Maxlen</th>
<th>Origin-AS</th>
<th>Source</th>
<th>Neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.232.0.0/16</td>
<td>32</td>
<td>10318</td>
<td>0</td>
<td>10.1.1.6/8282</td>
</tr>
<tr>
<td>31.3.8.0/21</td>
<td>21</td>
<td>5524</td>
<td>0</td>
<td>10.1.1.6/8282</td>
</tr>
<tr>
<td>31.7.8.0/21</td>
<td>21</td>
<td>8676</td>
<td>0</td>
<td>10.1.1.6/8282</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>217.198.192.0/20</td>
<td>20</td>
<td>197077</td>
<td>0</td>
<td>10.1.1.6/8282</td>
</tr>
<tr>
<td>217.199.224.0/20</td>
<td>24</td>
<td>25299</td>
<td>0</td>
<td>10.1.1.6/8282</td>
</tr>
<tr>
<td>217.224.0.0/11</td>
<td>11</td>
<td>3320</td>
<td>0</td>
<td>10.1.1.6/8282</td>
</tr>
</tbody>
</table>
```

test-rtr> sh ip bgp 93.175.146.0/24
BGP routing table entry for 93.175.146.0/24, version 8995350
Paths: (1 available, best #1, table default)
   Not advertised to any peer
   Refresh Epoch 1
64510 3333 12654, (received & used)
   10.1.1.5 from 10.1.1.2 (10.1.1.2)
   Origin IGP, localpref 110, valid, external, best path 51012284 RPKI State valid|
RPKI Operations: Route States

• **Valid**: the prefix-ASN pair has been found in the database
• **Invalid**: the prefix was found but with another ASN, or the prefix was found but the length is invalid (too long or too short)
• **Unknown / not found**: the prefix was not found
RPKI Operations: Route States

- Use route maps to manage route selection based on RPKI state:
  - `route map rpki-pref permit 10`
    `match rpki invalid`
    `set local-preference 90`
  - `route map rpki-pref permit 20`
    `match rpki not-found`
    `set local-preference 100`
  - `route map rpki-pref permit 30`
    `match rpki valid`
    `set local-preference 110`
- (The above also happens to be how the router will operate when allow-invalids has been enabled)
References

- https://www.apnic.net/community/security/
- RFC 6480: Resource Public Key Infrastructure
- RFC 3779: Extensions for IP addresses and ASNs