RPKI at IXP Route Servers

AfPIF, Mauritius
August 2019

Nick Hilliard

Chief Technical Officer
Internet Neutral Exchange Association CLG
ROAs - Route Origin Authorisations

- A cryptographically secure replacement for route[6] objects
- Adds maximum prefix length
- Yields route origin triplets that have been validated

(Origin AS, Prefix, Max Length)
(AS65500, 2001:db8::/32, /48)
(AS65501, 192.0.2.0/24, /24)
NEW ROUTE SERVERS

Route Server Refresh at INEX

- RPKI just one element
- Upgrade configuration from Bird v1.6 to Bird v2.0
- Complete rewrite of filtering workflow
  - Large communities used extensively within the route server
- Upgrade Bird's Eye\(^1\) for Bird v2 BGP
- Overhaul IXP Manager looking glass

1. A secure micro service for querying Bird - [https://github.com/inex/birdseye](https://github.com/inex/birdseye)
Bird v1 to v2 Changes

- RPKI-RTR supported
- Collapsed separate daemons for IPv4 and IPv6 into a single daemon
  - master route table becomes master4 / master6
  - new protocol blocks: ipv4 { ... } / ipv6 { ... }
- Other very minor configuration changes
Validating BGP Routing with RPKI-RTR

- A cache server (*validator*) does the cryptographic heavy lifting
- Routers receive and maintain the set of ROAs via RPKI-RTR from the cache
- RPKI gives three validation results: VALID, INVALID, UNKNOWN
NEW ROUTE SERVERS

IXP Manager v5 Route Server Filtering

1. Small prefixes (default is > /24 / /48 for ipv4 / ipv6)
2. Martians / bogons
3. Ensure at least 1 ASN and <= 64 ASNs in path
4. Ensure peer AS is the same as first AS in the prefix’s AS path
5. Prevent next-hop hijacking
6. Filter known transit networks
7. Ensure origin AS is in set of ASNs from member AS-SET
8. RPKI:
   • Valid -> accept
   • Invalid -> drop
9. RPKI Unknown -> revert to standard IRRDB prefix filtering
NEW ROUTE SERVERS

IXP Manager v5 Route Server Filtering

1. Small prefixes (default is > /24 / /48 for ipv4 / ipv6)
2. Martians / bogons
3. Ensure at least 1 ASN and <= 64 ASNs in path
4. Ensure peer AS is the same as first AS in the prefix’s AS path
5. Prevent next-hop hijacking

6. Filter known transit networks
7. Ensure origin AS is in set of ASNs from member AS-SET
8. RPKI:
   - Valid -> accept
   - Invalid -> drop
9. RPKI Unknown -> revert to standard IRRDB prefix filtering
NEW ROUTE SERVERS

Filter Known Transit Networks

```python
define TRANSIT_ASNS = [ 174,
  209,
  701,
  702,
  1239,
  1299,
  2914,
  3257,
  3320,
  3356,
  3549,
  3561,
  4134,
  5511,
  6453,
  6461,
  6762,
  7018 ];

# Cogent
# Qwest (HE carries this on IXPs IPv6 (Jul 12 2018))
# UUNET
# UUNET
# Sprint
# Telia
# NTT Communications
# GTT Backbone
# Deutsche Telekom AG (DTAG)
# Level3
# Level3
# Savvis / CenturyLink
# Chinanet
# Orange opentransit
# Tata Communications
# Zayo Bandwidth
# Seabone / Telecom Italia
# AT&T
```
NEW ROUTE SERVERS

IXP Manager v5 Route Server Filtering

1. Small prefixes (default is > /24 / /48 for ipv4 / ipv6)
2. Martians / bogons
3. Ensure at least 1 ASN and <= 64 ASNs in path
4. Ensure peer AS is the same as first AS in the prefix’s AS path
5. Prevent next-hop hijacking
6. Filter known transit networks
7. Ensure origin AS is in set of ASNs from member AS-SET
8. RPKI:
   • Valid -> accept
   • Invalid -> drop
9. RPKI Unknown -> revert to standard IRRDB prefix filtering
Ensure Origin AS is in member’s AS-SET

as-set: AS-HEANET
descr: Autonomous Systems routed by HEAnet
members: AS1213, AS2128, AS112, AS42310, AS2850, AS-IEDR
remarks: Group ASs routed by HEAnet together
mnt-by: HEANET-NOC
source: RIPE

No ability to create AS sets in RPKI

draft-ietf-grow-rpki-as-cones will resolve this

This is a regression over static IRRDB filtering

1. BGP filtering automation tool: https://github.com/snar/bgpq3
NEW ROUTE SERVERS

IXP Manager v5 Route Server Filtering

1. Small prefixes (default is > /24 / /48 for ipv4 / ipv6)
2. Martians / bogons
3. Ensure at least 1 ASN and <= 64 ASNs in path
4. Ensure peer AS is the same as first AS in the prefix’s AS path
5. Prevent next-hop hijacking
6. Filter known transit networks
7. Ensure origin AS is in set of ASNs from member AS-SET
8. RPKI:
   • Valid -> accept
   • Invalid -> drop
9. RPKI Unknown -> revert to standard IRRDB prefix filtering
NEW ROUTE SERVERS

IXP Manager v5 Bird Topology - Import From Member

AS112
BGP Peer

AS112
Routing Table

AS112
PIPE

Master RS
Routing Table

BGP import policy checks prefixes and tags them for later filtering

Pipe 'to master' filter filters all tagged prefixes
# Route Server BGP Community Usage

<table>
<thead>
<tr>
<th>Description</th>
<th>Large Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPKI Valid</td>
<td>43760:1000:1</td>
</tr>
<tr>
<td>RPKI Unknown</td>
<td>43760:1000:2</td>
</tr>
<tr>
<td>IRRDB Valid</td>
<td>43760:1001:1</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Large Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bogon Prefix</td>
<td>43760:1101:3</td>
</tr>
<tr>
<td>IRRDB Invalid</td>
<td>43760:1101:9</td>
</tr>
<tr>
<td>RPKI Invalid</td>
<td>43760:1101:13</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Side note: 43760:1101:* are filtered

NEW ROUTE SERVERS

IXP Manager v5 Bird Topology - Export To Member

Strip route server tags

Pipe 'from master' applies standard IX community filtering
### Standard IX Route Server Community Filters

<table>
<thead>
<tr>
<th>Description</th>
<th>Community</th>
<th>Large Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent announcement of a prefix to a certain peer</td>
<td>0:peer-as</td>
<td>43760:0:peer-as</td>
</tr>
<tr>
<td>Announce a prefix to a certain peer</td>
<td>43760:peer-as</td>
<td>43760:1:peer-as</td>
</tr>
<tr>
<td>Prevent announcement of a prefix to all peers</td>
<td>0:43760</td>
<td>43760:0:0</td>
</tr>
<tr>
<td>Announce a prefix to all peers</td>
<td>43760:43760</td>
<td>43760:1:0</td>
</tr>
</tbody>
</table>

**Side note**
RPKI Implementation Notes
Validator Software - RIPE NCC RPKI Validator 3

- RIPE NCC RPKI Validator 3 released in 2018
  - https://github.com/RIPE-NCC/rpki-validator-3
- Dramatically reduces installation complexity
- Modest VM requirements, runs on standard OS distributions
- Requirement to download ARIN TAL separately

```
$ tar zxf rpki-validator-latest-dist.tar.gz
$ ./rpki-validator-3.0-x/rpki-validator-3.sh
$ open http://localhost:8080

$ tar zxf rpki-rtr-server-latest-dist.tar.gz
$ ./rpki-rtr-server/rpki-rtr-server-3.sh
```
Validator Software - Routinator

- Routinator by NLnet Labs
  - https://github.com/NLnetLabs/routinator
- First impressions: low overhead, installation simplicity, stable, "just works"
- Requirement to download ARIN TAL separately

```bash
$ curl https://sh.rustup.rs -sSf | sh
$ source ~/.cargo/env
$ cargo install routinator
$ routinator rtrd -al 127.0.0.1:3323
```
roa4 table t_roa;

protocol rpki rpki1 {
    roa4 { table t_roa; }

    remote "192.0.2.67" port 3323;

    retry keep 90;
    refresh keep 900;
    expire keep 172800;
}

# RPKI check
rpki_result = roa_check( t_roa, net, bgp_path.last_nonaggregated );

if( rpki_result = ROA_INVALID ) then {
  ... 
}

# or ROA_VALID / ROA_UNKNOWN
Implementation Process at INEX

- INEX has two route servers and a route collector per LAN
- Upgrade route collector to Bird v2 + RPKI first
  - identify members who peer on the route server with RPKI invalid prefixes
  - found 4 members of ~80 with issues
    - 1 x more specific advertised than ROA allowed for
    - 1 x origin AS not matching ROA
    - 1 x member still advertising transferred space, new owners had ROAs
    - 1 x member created ROA for upstream peer-as rather than origin-as
  - members alerted to this on a "FYI basis" (i.e. non-blocking for INEX)
- Route server #1 completed Feb 7th
- Route server #2 completed Feb 14th
Implementation Process at INEX

- Outside of the four members with issues, no other member issues
- No issues to date with Bird v2
- Some issues with RIPE NCC Validator (crashing, disk space)
- No issues with Routinator
- There's a lot in this:
  - Bird v2
  - 24 route collectors and route servers
  - Large community tagging and filtering
  - RPKI vs IRRDB
  - etc
This is the public looking glass. Uncached results and additional routers available when logged in.

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Description</th>
<th>%</th>
<th>ASN</th>
<th>Table</th>
<th>PfxLimit</th>
<th>State/PfxRcd</th>
<th>PfxExp</th>
<th>%</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>185.1.69.6</td>
<td>AS1112 - AS1112 Reverse DNS</td>
<td>112</td>
<td>master4</td>
<td>2</td>
<td>596</td>
<td>0</td>
<td>Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>185.1.69.24</td>
<td>AS714 - Apple Distribution International</td>
<td>714</td>
<td>master4</td>
<td>597</td>
<td>0</td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>185.1.69.11</td>
<td>AS1213 - HEAnet</td>
<td>1213</td>
<td>master4</td>
<td>0</td>
<td>0</td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>185.1.69.12</td>
<td>AS5466 - Elr</td>
<td>5466</td>
<td>master4</td>
<td>77</td>
<td>0</td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>185.1.69.17</td>
<td>AS15405 - East Cork Broadband</td>
<td>15405</td>
<td>master4</td>
<td>5</td>
<td>0</td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>185.1.69.14</td>
<td>AS16171 - Strencom</td>
<td>16171</td>
<td>master4</td>
<td>4</td>
<td>0</td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>185.1.69.16</td>
<td>AS20940 - Akamai Technologies</td>
<td>20940</td>
<td>master4</td>
<td>1</td>
<td>0</td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>185.1.69.23</td>
<td>AS25152 - RIPE NCC k-root server</td>
<td>25152</td>
<td>master4</td>
<td>1</td>
<td>0</td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>185.1.69.18</td>
<td>AS3122 - Viatel</td>
<td>31122</td>
<td>master4</td>
<td>90</td>
<td>0</td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>185.1.69.19</td>
<td>AS41736 - Nova Telecom</td>
<td>41736</td>
<td>master4</td>
<td>3</td>
<td>0</td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>185.1.69.21</td>
<td>AS42090 - Rapid Broadband</td>
<td>42090</td>
<td>master4</td>
<td>6</td>
<td>0</td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Next Hop</td>
<td>Metric</td>
<td>Communities?</td>
<td>AS Path</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>------------</td>
<td>--------</td>
<td>--------------</td>
<td>------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>104.132.227.0/24</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1</td>
<td>5466 41264</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>109.125.0.0/18</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1</td>
<td>5466 15751</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>132.189.78.0/24</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1 ✓</td>
<td>5466 8116</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>132.189.79.0/24</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1 ✓</td>
<td>5466 8116</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>132.237.132.0/24</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1</td>
<td>5466 30614</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>132.237.167.0/24</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1</td>
<td>5466 30614</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>134.191.192.0/24</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1</td>
<td>5466 4983</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>134.191.216.0/22</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1</td>
<td>5466 4983 4983 4983 4983 4983 4983 4983 4983 4983 4983 4983 4983 4983</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>134.191.220.0/23</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1</td>
<td>5466 4983 4983 4983 4983 4983 4983 4983 4983 4983 4983 4983 4983 4983 4983</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>134.191.240.0/22</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1 ✓</td>
<td>5466 4983</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>134.191.244.0/24</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1 ✓</td>
<td>5466 4983</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>134.191.246.0/23</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1</td>
<td>5466 4983</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>135.74.153.0/24</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1 ✓</td>
<td>5466 18676</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>146.214.64.0/23</td>
<td>185.1.69.12</td>
<td>100</td>
<td>1 ✓</td>
<td>5466 42213</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Route Details - 132.189.78.0/24 as received from protocol pb_as5466_vli223_ipv4

<table>
<thead>
<tr>
<th><strong>Network</strong></th>
<th>132.189.78.0/24</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gateway</strong></td>
<td>185.1.69.12</td>
</tr>
<tr>
<td><strong>From Protocol</strong></td>
<td>pb_as5466_vli223_ipv4</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td>2019-02-12 09:12:03</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>100</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>BGP univ</td>
</tr>
<tr>
<td><strong>BGP :: AS Path</strong></td>
<td>5466 8116</td>
</tr>
<tr>
<td><strong>BGP :: Local Pref</strong></td>
<td>100</td>
</tr>
<tr>
<td><strong>BGP :: Communities</strong></td>
<td>5466:20</td>
</tr>
</tbody>
</table>
| **BGP :: Large Communities** | 2128:1000:2 | **APKIX UNKNOWN**  
|                | 2128:1101:9     | **IRAMO PREFIX FILTERED**  
|                | 2128:1001:1001  | **IRAMO FILTERED STRICT**  |

---

**INEX**
New Route Server Filtered Prefixes Tool

Your INEX - IXP Manager Dashboard

Aggregate Traffic Statistics

Recent Members
Our five most recent members are listed below. Have you arranged peering with them yet?
Route Server Filtered Prefixes

**Bad news!** We found 9 prefix(es) that are currently being filtered.

These are listed below with the reason for the filtering and the route server where filtering has been applied.

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Filtered Because</th>
<th>Filtered On Router(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>87.232.5.0/24</td>
<td>IRRDB PREFIX FILTERED</td>
<td>rs1-lan1-ipv4 rs2-lan1-ipv4</td>
</tr>
<tr>
<td>87.232.128.0/21</td>
<td>RPKI INVALID</td>
<td>rs1-lan1-ipv4 rs2-lan1-ipv4</td>
</tr>
<tr>
<td>87.232.64.0/18</td>
<td>NEXT HOP NOT PEER IP</td>
<td>rs1-lan1-ipv4 rs2-lan1-ipv4</td>
</tr>
<tr>
<td>87.232.32.0/19</td>
<td>RPKI INVALID</td>
<td>rs1-lan1-ipv4 rs2-lan1-ipv4</td>
</tr>
<tr>
<td>91.197.36.0/22</td>
<td>TRANSIT FREE ASN</td>
<td>rs1-lan1-ipv4 rs2-lan1-ipv4</td>
</tr>
</tbody>
</table>
IXP Manager v5.0 Released

- BIRD2 support for route servers, route collectors, AS112
- RPKI support
- Major looking-glass overhaul, including Prefix Analysis Tool
- Laravel upgrade for latest framework support
- Bootstrap upgrade with new front-end look
- Released in May 2019 on https://github.com/inex/IXP-Manager
THANK YOU

Any Questions?