Enhancing Route Origin Validation by Aggregating Validated ROA Payloads

draft-zhang-sidrops-vrp-aggregation-00

Jia Zhang, Mingwei Xu, Yangyang Wang

IETF 119 SIDROPS Meeting
Problem Statement
Is the `Invalid` BGP Route truly Invalid?

INVALID: > 40K BGP Routes

All route origin hijacking? NO!

Due to route aggregation, traffic engineering...

Prefix $\supseteq$ Prefix

In the BGP Route

In the ROA

Sometimes Valid

ROA Stats 2024-03-13
Problem Statement
Eg. Route-Aggregation-Caused Error Validation

Provider
AS11404

Customer
AS62915

BGP Route (76.191.64.0/18 AS11404) **Valid**

RPKI ROA (76.191.64.0/18 AS11404 24)

BGP Route (76.191.74.0/23 AS62915) **Valid**

(76.191.76.0/22 AS62915) **Invalid**

RPKI ROA (76.191.74.0/23 AS62915 24)

(76.191.76.0/23 AS62915 24)

(76.191.78.0/23 AS62915 24)

Should it be Valid?
Problem Statement

Eg. Traffic-Engineering-Caused Error Validation

Should it be Valid?

<table>
<thead>
<tr>
<th>RPKI ROA</th>
<th>(60.244.0.0/16</th>
<th>AS17709</th>
<th>17)</th>
</tr>
</thead>
</table>

| BGP Route | 60.244.0.0/18 | AS7482  | * 4637 17709 7482 |
|           | 60.244.0.0/18 | AS7482  | * 4780 17709x3 7482 |
|           | 60.244.0.0/16 | AS7482  | * 15412 17709x7 7482 |

<table>
<thead>
<tr>
<th>RPKI ROA</th>
<th>(60.244.0.0/17</th>
<th>AS7482</th>
<th>24)</th>
</tr>
</thead>
</table>

| RPKI ROA                     | (60.244.128.0/17  | AS7482 | 24) |
Yes! Those BGP Route should be validated as `Valid`.

• Main factor: Network routing policies or incomplete registration.
  • Which the address space holders are not aware of when issuing ROAs.

• Our solution

**Extend the Original VRPs by Generating Aggregated VRPs!**
Algorithm
Which VRPs Can Be Safely Aggregated?

Prefix
185.207.116.0/24
185.207.117.0/24
185.207.118.0/23

ASN
AS559
AS559
AS559

MaxLength
24
24
24

① Contiguous Prefix
② Same AS
③ Same MaxLength

❌ Overlap
❌ Gap
## Algorithm
### How to Aggregate?

<table>
<thead>
<tr>
<th>Prefix</th>
<th>ASN</th>
<th>MaxLength</th>
</tr>
</thead>
<tbody>
<tr>
<td>185.207.116.0/24</td>
<td>AS559</td>
<td>24</td>
</tr>
<tr>
<td>185.207.117.0/24</td>
<td>AS559</td>
<td>24</td>
</tr>
<tr>
<td>185.207.118.0/23</td>
<td>AS559</td>
<td>24</td>
</tr>
</tbody>
</table>

Largest parent prefix: **185.207.116.0/22**

Aggregated VRP: **185.207.116.0/22**
Algorithm
Is the aggregated VRP \textit{the same as} the original VRP?

\textbf{Reachability: Yes}

Route \((185.207.116.0/22, \text{AS599})\) \textcolor{red}{Reachable}

Route \((185.207.116.0/23, \text{AS599})\) \textcolor{red}{Reachable}

185.207.116.0/24 \quad 185.207.117.0/24 \quad 185.207.118.0/23

Reachable

Route \((185.207.116.0/24, \text{AS599})\)
(185.207.117.0/24, \text{AS599})
(185.207.118.0/23, \text{AS599})

 Authorized to originate

ROA \((185.207.116.0/24, \text{AS599}, 24)\)
(185.207.117.0/24, \text{AS599}, 24)
(185.207.118.0/23, \text{AS599}, 24)
Algorithm
Is the aggregated VRP the same as the original VRP?

Security: Yes

User -> Cloud
185.207.116.0/24
185.207.117.0/24
185.207.118.0/23
If Hijack 185.207.116.0/22

No Other traffic will be routed here!
**Algorithm**

Is the aggregated VRP **the same** as the original VRP?

<table>
<thead>
<tr>
<th>Usage for ROV: <strong>No</strong></th>
<th>VRPs</th>
<th>Prefix</th>
<th>ASN</th>
<th>MaxLength</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Original</strong></td>
<td>185.207.116.0/24</td>
<td>AS559</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>185.207.117.0/24</td>
<td>AS559</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>185.207.118.0/23</td>
<td>AS559</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td><strong>Aggregated</strong></td>
<td>185.207.116.0/22</td>
<td>AS559</td>
<td>24</td>
<td></td>
</tr>
</tbody>
</table>

When Update comes...

1. 185.207.116.0/23, AS559  **Valid**
2. 185.207.116.0/22, AS100  **Invalid**  ?? *Up to the original VRPs!!*
Implementation
Extension on the Router

Original VRP → VRP Aggregation → Aggregated VRP

Update
Validity State = NULL

Update
Validity State = U/I

Update
Validity State unchanged

ASBR
• Questions, criticisms, and applause are welcome.
• Further discussion is needed.
  • Implementation
    • Is router modification the most practical solution?
    • Or should we consider more extensive architectural modification?
  • Incremental Aggregation
Thank you!

Enhancing Route Origin Validation by Aggregating Validated ROA Payloads

IETF 119 SIDROPS Meeting

zhangj@mail.zgclab.edu.cn