Signaling Prefix Origin Validation Results from an RPKI Origin Validating BGP Speaker to BGP Peers

draft-ietf-sidrops-validating-bgp-speaker
IETF 105, July 23 2019, Montreal
Timeline

2015-12 first version
draft-kklf-sidr-route-server-rpki-light

2017-04 added modes of operation

2018-01 swapped RFC8097 community to EBGP Prefix Origin Validation Extended Community

Included feedback from IETF104 meeting
Motivation

- Mimic RFC8097 (IBGP only) for IXPs
- Forward RPKI origin validation results with IBGP

- Natural for IXPs to forward routing details to peers to:
  - make routing decisions
  - monitoring, maintenance, troubleshooting
  - educational and research purposes
Signaling at an IXP

AS B

AS C

AS D

AS Y

AS Z

IXP

RS

RPKI enabled Route Server

Signaling Prefix Origin Validation Results to Peers
draft-ietf-sidrops-validating-bgp-speaker
Current Implementation

Transitive 12-octet AS Specific Large Community (RFC8092 & RFC8195):

1. ROA validity status of a prefix (Local Administrator field)
2. Function specific value TBD (Local Data Part 1)
3. Signaling ASN (Local Data Part 2)
Modes of operation

Allow for 3 modes of operation for validating BGP speaker:

1. **Tag prefixes** with their ROA validity status, and advertise them.
2. **Drop prefixes with ROA status "Invalid"** (default mode)
   Tag the remaining "Unknown" and "Valid" routes, and advertise them.
3. **Drop prefixes with ROA status "Invalid" and "Unknown"**
   Tag the remaining "Valid" routes, and advertise them.
Operational Recommendations

- Peers can **redistribute**, but **only in their own AS**
- A route server must strip a similar community at reception
- In case of **failure in the origin validation** check → **community omitted**
- If a peer obtained multiple validations states, they should only use the highest value
Past Comments

- **Signaling if validation wasn’t performed**
  - Operational recommendation omitting community tag completely

- **Draft overtaken by reality**
  - Dropping of invalids by default is getting common at IXPs

- **Extended community vs. large community**
  - Changed from extended to large communities

- **Concern of outsourcing security**
  - Common and a trade-off in the Peer→ IXP relationship

- **Drop invalids as default mode of operation in this draft**
  - Now adopted in the draft