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

draft-ietf-sidrops-validating-bgp-speaker-02
IETF 101, March 22 2018, London
Primary Goals of this I-D

● Lower the barrier of entry, e.g. for customers who are reluctant in dipping their toes, due to political, technical or business reasons.

● Standardize the way BGP speakers (e.g. IXP route servers) communicate ROA validation status via BGP communities.
Signaling at an IXP

RPKI enabled Route Server
Signaling Prefix Origin
Validation Results to Peers

draft-ietf-sidrops-validating-bgp-speaker-02
Brief I-D History

2017-01: -00 released
2017-01: -01 released (migration from SIDR to SIDRops)
2017-04: -02 released (addition of operation modes, reference updates, cosmetic changes)
2018-01: -00 of draft-ietf-sidrops-validating-bgp-speaker released (route server => BGP speaker, swap RFC8097 community to ad-hoc EBGP Prefix Origin Validation Extended Community)
2018-02: -01 released (minor typo fixed)
2018-03: -02 released (simplified language, added further clarifications, fixed more typos)
Method of standardization

Introduce a transitive four-octet AS Specific Extended Community, which signals:

1. ROA validity status of a prefix (Local Administrator field)
2. Signaling ASN (Global Administrator field)
Method of standardization (cont'd)

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"**. Tag the remaining "Unknown" AKA "NotFound" and "Valid" routes, and advertise them.
3. **Drop prefixes with ROA status "Invalid" or "Unknown"**. Tag the remaining "Valid" routes, and advertise them.
Path hiding concerns

- ROA validity of prefixes is just another input for per-client policy controls, as described in §2.3.1 and addressed in §2.3.2 of RFC 7947 (multiple RIBs, ADD-PATH, etc.). In that case, BGP best path selection algorithm will run after dropping "Invalids" (mode 2) or "Invalids" and "Unknowns" (mode 3).
- Furthermore, at least one implementation used in IXPs supports sending the next best available path.
- This means that no path hiding will occur, if so desired, but can still be an option for operators, e.g. when having routes obtained via other peers.
Security and/or operational concerns

- Draft is addressing *technical* concerns and describing all available options, having the primary goals (presented in slide 2) in mind. Operational and security (best) practices are left to the operator, or other drafts.