

Export of BGP Prefix Origin Validation in IPFIX

draft-liu-opsawg-ipfix-bgp-pov-02

Yisong Liu China Mobile

Xueyan Song ZTE Corp.

Taoran zhou ZTE Corp.

IETF 126, Vienna

Overview

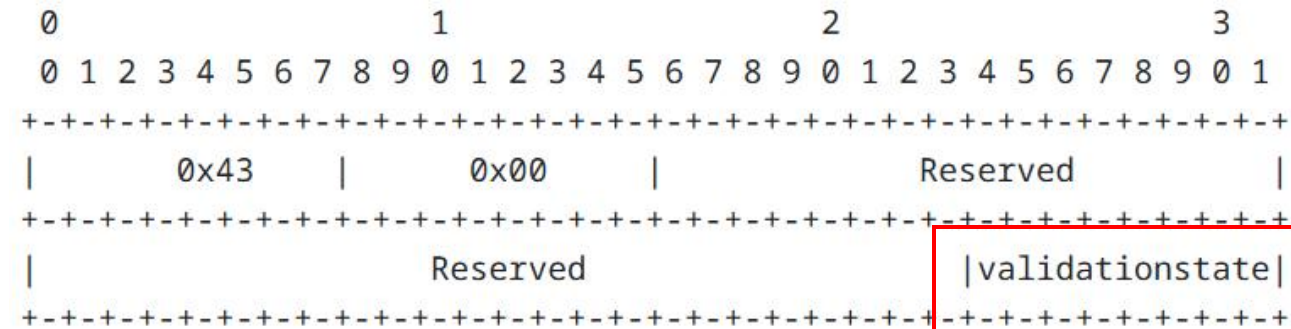
- **RFC 6811** defines the BGP Prefix Origin Validation mechanism, which leverages the security of the RPKI database to verify whether the origin AS of a BGP route is legitimate, helping to prevent route hijacking and misconfiguration to a certain extent.
- The **purpose** of this document is to define an IPFIX Information Element to enable network operators to collect and analyze BGP route validation states (valid, invalid, not found) to facilitate the detection of potential route hijacks improving network observability and security.

Values

- Address the **gap** in current IETF standards for monitoring the POV validation state of BGP routes within a network.
- Enhance **network observability** by transforming the local validation state of BGP routers into IPFIX export data.
- Enable operators to detect potential route hijacks and improve **network security**.

IPFIX Information Element

- **Name:** bgpPrefixOriginValidationState
- **Description:** The validation state value is carried in an unsigned integer, using code points aligned with for the validation outcomes.
 - 0: valid - At least one Validated ROA Payload (VRP) matches the route prefix and origin AS.
 - 1: not found - No VRP covers the route prefix.
 - 2: invalid - At least one VRP covers the route prefix, but no VRP matches it.



Value	Meaning
0	Lookup result = "valid"
1	Lookup result = "not found"
2	Lookup result = "invalid"

Feedback and Updates – 1/3

- **Thanks to Jeff for comments on IE desgins:**

- **IE code points** SHOULD follow RFC 8097 to avoid unnecessary divergence. This would make the IE carry a uint8 rather than a bit vector.
- Suggest **NOT** specifying "no origin validation is done" as you have with value 0. The absence of this IE is sufficient for that state.
- **Should specify** which BGP Routes are used for reporting. conventionally this is the **active route** (i.e., the LocRIB entry).
- **RFC 8893**, which this document cannot support, highlights how validation state may vary depending on perspective.

- **Draft v01 updates:**

- **Modified the IE description** to include an explanation of the IE value, with reference to the definitions in RFC 8097.
- **Changed the data format** of the IE value to unsigned8, rather than a bit vector.
- **Added a reference to RFC 8893** to clarify that the information extracted by the IE is the result of this RPKI application policy.
- **Added deployment considerations** for scenarios where the BGP POV validation function is not enabled or the route is non-active.

Feedback and Updates – 2/3

- **Thanks to Chongfeng for comments on relationship with existing IEs:**

- Whether the monitoring of BGP Prefix Validation state is related to “**traffic flow**”. How to define the “traffic flow” in the case.
- Why not use the existing “IPFIX Information Element bgpValidityState (Element **ID 294**, see IANA-IPFIX).

- **Draft v01 updates:**

- **Validation state** is obtained by comparing BGP Update prefix/AS with the local RPKI VRP cache, then exported to the IPFIX collector.
- Valid BGP routes correspond to **traffic flows** derived from those routes; the exported BGP POV validation state serves as a route validity attribute for the corresponding BGP flows.
- **ID 294** defines the validation field per RFC 8097. Our draft incorporates Jeff’s suggestions and **takes RFC 8893** (an enhancement to RFC 6811) into account.
- Our draft focuses on **comparison/verification between local BGP POV and RPKI**, which is distinct from the issues addressed by ID 294.

Feedback and Updates – 3/3

- **Thanks to Haiyang and Jeff for scope clarification:**

- Regarding the **monitoring coverage** of the proposed IPFIX IE. RFC 8097 defines the RPKI validation state as an Extended Community attached to BGP route attributes, which could apply to all received BGP routes.
- Information of ECMP by a BGP speaker is often quite proprietary, with less value for standardization.

- **Draft v02 updates:**

- The IE is scoped to the **LocRIB** simply because IPFIX exporters typically monitor installed forwarding state, not all received routes.
- Added clarifications on the **scope**:
*...the validation state exported by this Information Element reflects only the **active forwarding route** selected for the observed traffic. **Inactive routes, backup routes, and routes not selected** by the forwarding engine are **outside the scope** of this document...*

Next Steps

- Welcome review, comments and questions
- Request WG Adoption