OPSAWG
Internet-Draft
Intended status: Standards Track
Expires: 14 August 2026

Y. Liu
China Mobile
X. Song
T. Zhou
ZTE Corporation

10 February 2026

Export of BGP Prefix Origin Validation in IP Flow Information Export (IPFIX)

draft-liu-opsawg-ipfix-bgp-pov-00

Abstract

This document defines an IP Flow Information Export (IPFIX) Information Element for monitoring the state of Resource Public Key Infrastructure (RPKI) based BGP Prefix Origin Validation. The Information Element enables 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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 14 August 2026.

Copyright Notice

Table of Contents

1. Introduction

The RPKI [RFC6480] provides a cryptographic framework for validating the association between IP address blocks and Autonomous System (AS) numbers. BGP Prefix Origin Validation, as defined in [RFC6811], enables routers to verify whether the origin AS of a BGP route announcement is authorized to advertise the corresponding IP prefix, based on Route Origin Authorizations (ROAs) [RFC9582] in the RPKI.

When BGP Prefix Origin Validation is enabled on a router, the router maintains a local cache of Validated ROA Payloads (VRPs) obtained through the RPKI-to-Router protocol (RTR) [RFC8210]. For each received BGP UPDATE message, the router extracts the announced IP prefix and its origin AS, compares this tuple against the local VRP cache, and assigns a validation state (valid, invalid, not-found) according to the algorithm specified in [RFC6811]. This validation state can be attached as a local path attribute to the BGP route entry and influence subsequent routing decisions, such as route filtering and route preference adjustment.

While this validation mechanism enhances BGP security, network operators currently lack standardized methods to monitor the validation states across their network infrastructure. IP Flow Information Export (IPFIX) [RFC7011] provides a standard protocol for exporting flow information from network devices. There is an existing IPFIX Information Element bgpValidityState (Element ID 294, see IANA-IPFIX), which defines the "validity state" of the BGP route correspondent source or destination IP address. This element does not specifically address RPKI-based origin validation.

This document defines a new IPFIX Information Element specifically designed for monitoring the state of RPKI-based BGP Prefix Origin Validation. The element enables network operators to collect, analyze, and monitor the validation states of BGP routes across their network infrastructure.

2. Terminology

2.1. Terms Used in This Document

This document uses the following terms defined in [RFC6811].

Validated ROA Payload (VRP): A locally stored object which contains the content (IP address, prefix length, maximum length, origin AS number).

Prefix: (IP address, prefix length), interpreted as is customary (see [RFC4632]).

Route: Data derived from a received BGP UPDATE, as defined in [RFC4271].

Additionally, this document uses the terms defined in [RFC7011].

Observation Point: An Observation Point is a location in the network where packets can be observed. Examples include a line to which a probe is attached; a shared medium, such as an Ethernet-based LAN; a single port of a router; or a set of interfaces (physical or logical) of a router.

Exporter: A device that hosts one or more Exporting Processes is termed an Exporter.

IPFIX Device: An IPFIX Device hosts at least one Exporting Process. It may host further Exporting Processes as well as arbitrary numbers of Observation Points and Metering Processes.

Information Element: An Information Element is a protocol and encoding independent description of an attribute that may appear in an IPFIX Record. Information Elements are defined in the IANA "IPFIX Information Elements" registry (see IANA-IPFIX). The type associated with an Information Element indicates constraints on what it may contain and also determines the valid encoding mechanisms for use in IPFIX.

Exporting Process: The Exporting Process sends IPFIX Messages to one or more Collecting Processes. The Flow Records in the Messages are generated by one or more Metering Processes.

Collecting Process: A Collecting Process receives IPFIX Messages from one or more Exporting Processes. The Collecting Process might process or store Flow Records received within these Messages, but such actions are out of scope for this document.

2.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. IPFIX IEs for BGP Prefix Origin Validation

This section defines a new IPFIX Information Element for monitoring RPKI-based BGP Prefix Origin Validation.

3.1. bgpPrefixOriginValidationState

Name: bgpPrefixOriginValidationState

ElementID: TBD1

Description: It indicates the validation state of a BGP route prefix and its origin ASN as determined by BGP Prefix Origin Validation as defined in [RFC6811].

This element describes the result of comparing a BGP route prefix derived from a BGP UPDATE message against VRP obtained from RPKI server. The validation algorithm follows RFC6811.

The state of BGP Prefix Origin Validation is encoded in a single octet, where only the two latest significant bits (bits 0 and 1) are used. The four possible state are:

00: BGP Prefix Origin Validation is not enabled on the exporting device for this prefix. This indicates the administrative state where validation is inactive (e.g., not configured).

01: The validation state for the route prefix is valid. The state means at least one VRP matches the route prefix.

10: The validation state for the route prefix is invalid. The state means at least one VRP covers the route prefix, but no VRP matches it.

11: The validation state for the route prefix is not found. This state means no VRP covers the route prefix.

Bits 2 to 7 are reserved. The Exporting Process MUST set these bits to zero. The Collecting Process MUST ignore them.

Abstract Data Type: unsigned8

Data Type Semantics: identifier

Additional Information: See [RFC6811] the definition of validation state of BGP route prefix.

Reference: [RFC6811], this document.

4. Operational Considerations

The Observation Point [RFC7011] for monitoring BGP Prefix Origin Validation states is typically the router performing the validation. The router acting as an IPFIX Exporter is expected to have BGP Prefix Origin Validation enabled and properly configured. This includes establishing RTR sessions with RPKI cache servers and ensuring the local VRP cache is synchronized.

When network operators design a template for IPFIX export of BGP Prefix Origin Validation information export, which should combine with other context informations, such as sourceIPv4Prefix/ sourceIPv6Prefix, sourceIPv4PrefixLength/sourceIPv6PrefixLength, bgpSourceAsNumber, as defined in [RFC7012].

In scenarios of network changes or maintenance, frequent export of IPFIX records for BGP validation states may lead to considerable overhead on router resources and bandwidth. Operators should balance monitoring needs with performance impact by using thresholds, adjusted export intervals, or focused sampling, such as prioritizing invalid states, refer to [RFC5475] for sampling and filtering strategies.

5. Security Considerations

The security considerations for IPFIX in general discussed in [RFC7011], and those for RPKI and BGP Prefix Origin Validation discussed in [RFC6811] apply to this document.

The IPFIX data records containing BGP Prefix Origin Validation state SHOULD be transported using security protocols (such as TLS, DTLS) and satisfy the mutual authentication between IPFIX Exporting Processes and IPFIX Collecting Processes as specified in [RFC7011]. An implementation may use BGP Prefix Origin Validation state as the information input for network routing policies. Network operators should ensure that the data collection and storage of BGP Prefix Origin Validation state comply with applicable privacy regulations.

6. IANA Considerations

IANA is requested to assign a new Information Element ID in the IPFIX Information Elements registry.

Information Element bgpPrefixOriginValidationState with Element ID TBD1.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <https://www.rfc-editor.org/info/rfc6811>.

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <https://www.rfc-editor.org/info/rfc7011>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

7.2. Informative References

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", BCP 122, RFC 4632, DOI 10.17487/RFC4632, August 2006, <https://www.rfc-editor.org/info/rfc4632>.

[RFC5475] Zseby, T., Molina, M., Duffield, N., Niccolini, S., and F. Raspall, "Sampling and Filtering Techniques for IP Packet Selection", RFC 5475, DOI 10.17487/RFC5475, March 2009, <https://www.rfc-editor.org/info/rfc5475>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

[RFC7012] Claise, B., Ed. and B. Trammell, Ed., "Information Model for IP Flow Information Export (IPFIX)", RFC 7012, DOI 10.17487/RFC7012, September 2013, <https://www.rfc-editor.org/info/rfc7012>.

[RFC8210] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1", RFC 8210, DOI 10.17487/RFC8210, September 2017, <https://www.rfc-editor.org/info/rfc8210>.

[RFC9582] Snijders, J., Maddison, B., Lepinski, M., Kong, D., and S. Kent, "A Profile for Route Origin Authorizations (ROAs)", RFC 9582, DOI 10.17487/RFC9582, May 2024, <https://www.rfc-editor.org/info/rfc9582>.

Authors' Addresses

Yisong Liu
China Mobile
China
Email: liuyisong@chinamobile.com

Xueyan Song
ZTE Corporation
China
Email: song.xueyan2@zte.com.cn

Taoran Zhou
ZTE Corporation
China
Email: zhou.taoran@zte.com.cn