Stream: Internet Engineering Task Force (IETF)
RFC: 9565
Obsoletes: 7125
Category: Standards Track
Published: March 2024
ISSN: 2070-1721
Author: M. Boucadair
Orange

RFC 9565
An Update to the tcpControlBits IP Flow Information Export (IPFIX) Information Element

Abstract

RFC 7125 revised the tcpControlBits IP Flow Information Export (IPFIX) Information Element that was originally defined in RFC 5102 to reflect changes to the TCP header control bits since RFC 793. However, that update is still problematic for interoperability because some flag values have subsequently been deprecated.

This document removes stale information from the IANA "IPFIX Information Elements" registry and avoids future conflicts with the authoritative IANA "TCP Header Flags" registry.

This document obsoletes RFC 7125.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9565.

Copyright Notice

Table of Contents

1. Introduction

TCP defines a set of control bits (also known as "flags") for managing connections (Section 3.1 of [RFC9293]). The "TCP Header Flags" registry was initially set by [RFC3168], but it was populated with only TCP control bits that were defined in [RFC3168]. [RFC9293] fixed that by moving that registry to be listed as a subregistry under the "Transmission Control Protocol (TCP) Parameters" registry [TCP-FLAGS], adding bits that had previously been specified in [RFC0793], and removing the NS (Nonce Sum) bit per [RFC8311]. Also, Section 6 of [RFC9293] introduces "Bit Offset" to ease referencing each header flag's offset within the 16-bit aligned view of the TCP header (Figure 1 of [RFC9293]). [TCP-FLAGS] is thus settled as the authoritative reference for the assigned TCP control bits.

Note: The bits in offsets 0 through 3 are not header flags, but the TCP segment Data Offset field.

[RFC7125] revised the tcpControlBits IP Flow Information Export (IPFIX) Information Element that was originally defined in [RFC5102] to reflect changes to the TCP control bits since [RFC0793]. However, that update is still problematic for interoperability because a value was deprecated since then (Section 7 of [RFC8311]), and, therefore, [RFC7125] risks deviating from the authoritative "TCP Header Flags" registry [TCP-FLAGS].

This document fixes that problem by removing stale information from the "IPFIX Information Elements" registry [IPFIX] and avoiding future conflicts with the authoritative "TCP Header Flags" registry [TCP-FLAGS]. The update in this document also enhances observability. For example, network operators can identify packets that are observed with unassigned TCP flags set and, therefore, identify which applications in the network should be upgraded to reflect the changes to TCP flags that were introduced, e.g., in [RFC8311].

The main changes from [RFC7125] are listed in Appendix A.

2. Terminology

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.

This document uses the terms defined in Section 2 of [RFC7011].

3. Revised tcpControlBits Information Element

ElementID: 6

Name: tcpControlBits

Abstract Data Type: unsigned16

Data Type Semantics: flags

Status: current

Description: TCP control bits observed for the packets of this Flow. This information is encoded as a bit field; each TCP control bit has a corresponding bit in that field. A bit is set to 1 if any observed packet of this Flow has the corresponding TCP control bit set to 1. The bit is cleared to 0 otherwise.

Per [RFC9293], the assignment of TCP control bits is managed by IANA via the "TCP Header Flags" registry [TCP-FLAGS]. Implementers can retrieve the current TCP control bits from that registry, which is authoritative for them.

As the most significant 4 bits of octets 12 and 13 (counting from zero) of the TCP header [RFC9293] are used to encode the TCP data offset (header length), the corresponding bits in this Information Element **MUST** be reported by the Exporter with a value of zero and **MUST** be ignored by the Collector. Use the tcpHeaderLength Information Element to encode this value.

All TCP control bits (including those unassigned) **MUST** be exported as observed in the TCP headers of the packets of this Flow.

If exported as a single octet with reduced-size encoding (Section 6.2 of [RFC7011]), this Information Element covers the low-order octet of this field (i.e., bit offset positions 8 to 15) [TCP-FLAGS]. A Collector receiving this Information Element with reduced-size encoding must not assume anything about the content of the four bits with bit offset positions 4 to 7.

Exporting Processes exporting this Information Element on behalf of a Metering Process that is not capable of observing any of the flags with bit offset positions 4 to 7 **SHOULD** use reduced-size encoding, and only export the least significant 8 bits of this Information Element.

Note that previous revisions of this Information Element's definition specified that flags with bit offset positions 8 and 9 must be exported as zero, even if observed. Collectors should therefore not assume that a value of zero for these bits in this Information Element indicates the bits were never set in the observed traffic, especially if these bits are zero in every Flow Record sent by a given Exporter.

Note also that the "TCP Header Flags" registry [TCP-FLAGS] indexes the bit offset from the most significant bit of octet 12 to the least significant bit of octet 13 in the TCP header, but the tcpControlBits is encoded as a regular unsigned 16-bit integer.

Units:

Range:

Additional Information: See the assigned TCP control bits in the "TCP Header Flags" registry [TCP-FLAGS].

Reference: [RFC9293], RFC 9565

Revision: 2

4. An Example

Figure 1 shows an example of a tcpControlBits Information Element set to 0x92, where MSB indicates the most significant bit and LSB indicates the least significant bit. This Information Element is used to report TCP control bits for a Flow that has CWR (Congestion Window Reduced), ACK, and SYN flag bits set (that is, bit offset positions 8, 11, and 14).

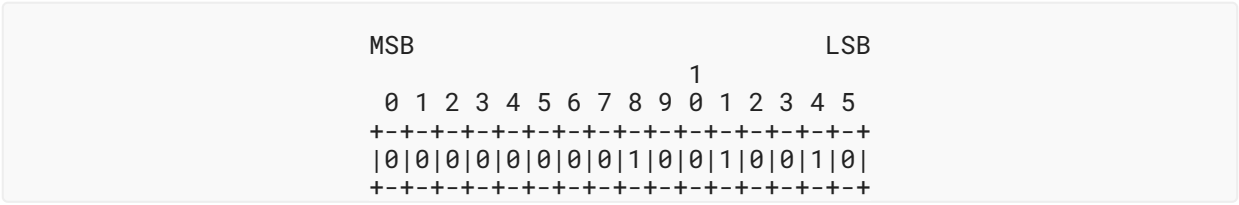

Figure 1: An Example of the tcpControlBits Information Element

5. IANA Considerations

IANA has updated the "tcpControlBits" entry of the "IPFIX Information Elements" registry [IPFIX] to echo the details provided in Section 3.

6. Security Considerations

Because the setting of TCP control bits may be misused in some Flows (e.g., Distributed Denial-of-Service (DDoS) attacks), an Exporter has to report all observed control bits even if no meaning is associated with a given TCP flag. This document uses a stronger requirements language compared to [RFC7125].

This document does not add new security considerations to those already discussed for IPFIX in [RFC7011].

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>.

[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>.

[RFC9293] Eddy, W., Ed., "Transmission Control Protocol (TCP)", STD 7, RFC 9293, DOI 10.17487/RFC9293, August 2022, <https://www.rfc-editor.org/info/rfc9293>.

[TCP-FLAGS] IANA, "TCP Header Flags", <https://www.iana.org/assignments/tcp-parameters/>.

7.2. Informative References

[IPFIX] IANA, "IPFIX Information Elements", <https://www.iana.org/assignments/ipfix/>.

[RFC0793] Postel, J., "Transmission Control Protocol", RFC 793, DOI 10.17487/RFC0793, September 1981, <https://www.rfc-editor.org/info/rfc793>.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, DOI 10.17487/RFC3168, September 2001, <https://www.rfc-editor.org/info/rfc3168>.

[RFC5102] Quittek, J., Bryant, S., Claise, B., Aitken, P., and J. Meyer, "Information Model for IP Flow Information Export", RFC 5102, DOI 10.17487/RFC5102, January 2008, <https://www.rfc-editor.org/info/rfc5102>.

[RFC7125] Trammell, B. and P. Aitken, "Revision of the tcpControlBits IP Flow Information Export (IPFIX) Information Element", RFC 7125, DOI 10.17487/RFC7125, February 2014, <https://www.rfc-editor.org/info/rfc7125>.

[RFC8311] Black, D., "Relaxing Restrictions on Explicit Congestion Notification (ECN) Experimentation", RFC 8311, DOI 10.17487/RFC8311, January 2018, <https://www.rfc-editor.org/info/rfc8311>.

[RFC9487] Graf, T., Claise, B., and P. Francois, "Export of Segment Routing over IPv6 Information in IP Flow Information Export (IPFIX)", RFC 9487, DOI 10.17487/RFC9487, November 2023, <https://www.rfc-editor.org/info/rfc9487>.

Appendix A. Changes from RFC 7125

- Cleaned up the description of the tcpControlBits Information Element by removing mentions of stale flag bits, referring to the flag bits by their bit offset position, and relying upon the IANA "TCP Header Flags" registry.
- Removed the table of TCP flag bits from the description of the tcpControlBits Information Element.
- Added the reference [TCP-FLAGS] to the Additional Information field of the tcpControlBits Information Element.
- Used strong normative language for exporting observed flags.
- Updated the references of the tcpControlBits Information Element.
- Bumped the revision of the tcpControlBits Information Element.
- Replaced obsolete RFCs (e.g., [RFC0793]).
- Added an example section (Section 4).

Acknowledgments

This document was triggered by a discussion in the opsawg working group between the author and the authors of [RFC9487].

Thanks to Christian Jacquenet, Thomas Graf, and Benoît Claise for the review and comments.

Thanks to Michael Scharf for the tsvart review, Ketan Talaulikar for the rtgdir review, and Elwyn Davies for the genart review.

Thanks to Rob Wilton for the AD review.

Thanks to Tim Bray for the artart review and Shawn Emery for the secdir review.

Thanks to Éric Vyncke and Paul Wouters for the comments in the IESG review.

Acknowledgments from RFC 7125

Thanks to Andrew Feren, Lothar Braun, Michael Scharf, and Simon Josefsson for comments on the revised definition. This work is partially supported by the European Commission under grant agreement FP7-ICT-318627 mPlane; this does not imply endorsement by the Commission.

Contributors

The authors of [RFC7125] are as follows:

Brian Trammell

Paul Aitken

Author's Address

Mohamed Boucadair
Orange
35000 Rennes
France
Email: mohamed.boucadair@orange.com