Workgroup: Operations and Management Area
Internet-Draft:
draft-boucadair-opsawg-rfc7125-update-01
Updates: 7125 (if approved)
Published: 20 September 2022
Intended Status: Informational
Expires: 24 March 2023
Authors: M. Boucadair
Orange

# 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 Flags header field since RFC 793. However, that update is still problematic for interoperability because some values were deprecated since then.

This document updates RFC 7125 by removing stale information from the IPFIX registry and avoiding conflicts with the authoritative TCP registry.

## 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 24 March 2023.

## Copyright Notice

**Table of Contents**



## 1. Introduction

TCP defines a set of control bits (also known as "flags") for managing connections. The "Transmission Control Protocol (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, adding bits that had previously been specified in [RFC0793], and removing the NS (Nonce Sum) bit as per [RFC8311]. Also, [RFC9293] introduces "Bit Offset" to ease referencing each header flag's offset within the 16-bit aligned view of the TCP header (Section 3.1 of [RFC9293]). [TCP-FLAGS] is thus settled as the authoritative reference for the assigned TCP control bits.

[RFC7125] revised the tcpControlBits IP Flow Information Export (IPFIX) Information Element that was originally defined in [RFC5102] to reflect changes to the TCP Flags header field 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 to deviate from the authoritative registry [TCP-FLAGS].

This document fixes that problem by removing stale information from the IPFIX registry and avoiding future conflicts with the authoritative TCP registry. Also, because the setting of control bits may be misused in some flows (e.g., DDoS attacks), an exporter has to report all observed control bits even if no meaning is

currently associated with a given flag. This document uses a stronger requirement language compared to [RFC7125]. See Section 3 for more details.

## 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.

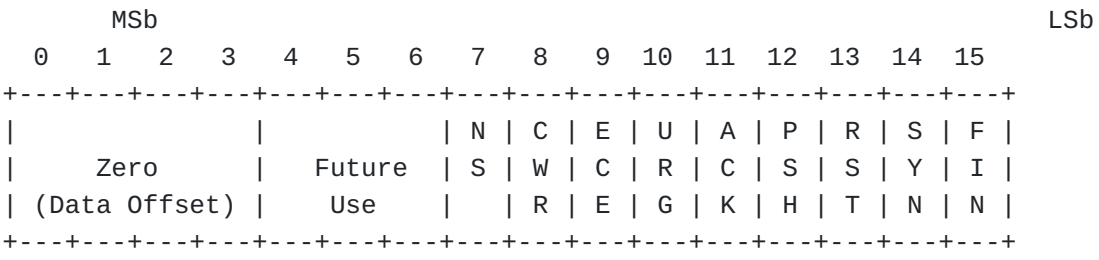
This document uses the terms defined in Section 2 of [RFC7011].

## 3. An Update to tcpControlBits IP Flow Information Export (IPFIX) Information Element

This document updates Section 3 of [RFC7125] as follows:

**OLD:**

The values of each bit are shown below, per the definition of the bits in the TCP header [RFC0793][RFC3168] [RFC3540]:




| bit value | flag name | description |
|---|---|---|
| 0x8000 | | Zero (see tcpHeaderLength) |
| 0x4000 | | Zero (see tcpHeaderLength) |
| 0x2000 | | Zero (see tcpHeaderLength) |
| 0x1000 | | Zero (see tcpHeaderLength) |
| 0x0800 | | Future Use |
| 0x0400 | | Future Use |
| 0x0200 | | Future Use |
| 0x0100 | NS | ECN Nonce Sum |
| 0x0080 | CWR | Congestion Window Reduced |
| 0x0040 | ECE | ECN Echo |
| 0x0020 | URG | Urgent Pointer field significant |
| 0x0010 | ACK | Acknowledgment field significant |
| 0x0008 | PSH | Push Function |
| 0x0004 | RST | Reset the connection |
| 0x0002 | SYN | Synchronize sequence numbers |
| 0x0001 | FIN | No more data from sender |

As the most significant 4 bits of octets 12 and 13 (counting from zero) of the TCP header [RFC0793] are used to encode the TCP data offset (header length), the corresponding bits in this Information Element MUST be exported as zero and MUST be ignored by the collector. Use the tcpHeaderLength Information Element to encode this value.

Each of the 3 bits (0x800, 0x400, and 0x200), which are reserved for future use in [RFC0793], SHOULD be exported as observed in the TCP headers of the packets of this Flow.

**NEW:**

As per [RFC9293], the assignment of the TCP control bits is managed by IANA from the "TCP Header Flags" registry [TCP-FLAGS]. That registry is authoritative to retrieve the most recent TCP control bits.

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 exported as zero and MUST be ignored by the collector. Use the tcpHeaderLength Information Element to encode this value.

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

## 4. IANA Considerations

IANA is requested to update the "tcpControlBits" entry of the [IPFIX] as follows:

*Update the description of to reflect the change in Section 3.

*Add [TCP-FLAGS] to the Additional Information field.

*Add this document to the references

## 5. Security Considerations

This document does not add new security considerations to those already discussed in Section 5 of [RFC7125].

## 6. Acknowledgements

This document was triggered by a discussion in opswag with the authors of draft-ietf-opsawg-ipfix-srv6-srh.

# 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>.

**[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>.

**[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/tcp-parameters.xhtml#tcp-header-flags>.


## 7.2. Informative References


**[IPFIX]** IANA, "IP Flow Information Export (IPFIX) Entities", <https://www.iana.org/assignments/ipfix/ipfix.xhtml>.

**[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>.

**[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>.

## Author's Address

Mohamed Boucadair
Orange
35000 Rennes
France

Email: mohamed.boucadair@orange.com