

IPFIX Working Group
Internet-Draft
Intended status: Informational
Expires: June 7, 2014

B. Trammell
ETH Zurich
P. Aitken
Cisco Systems, Inc
December 4, 2013

**Revision of the tcpControlBits IPFIX Information Element
draft-trammell-ipfix-tcpcontrolbits-revision-05.txt**

Abstract

This document revises the tcpControlBits IPFIX Information Element as originally defined in [[RFC5102](#)] to reflect changes to the TCP Flags header field since [[RFC0793](#)].

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 <http://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 June 7, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

1. Introduction

Octets 12 and 13 (counting from zero) of the TCP header encode the data offset (header length) in four bits, as well as 12 bits of flags. The least significant 6 bits of these were defined in [\[RFC0793\]](#) as URG, ACK, PSH, RST, SYN, and FIN for TCP control. Subsequently, [\[RFC3168\]](#) defined the CWR and ECE flags for Explicit Congestion Notification (ECN) negotiation and signaling; [\[RFC3540\]](#) additionally defined the NS flag for the ECN Nonce Sum.

As defined in the IANA IPFIX Information Element Registry [\[IANA-IPFIX\]](#), taken from [\[RFC5102\]](#), the tcpControlBits Information Element for IPFIX [\[RFC7011\]](#) only covers the original six bits from [\[RFC0793\]](#). To allow IPFIX to be used to measure the use of ECN, and to bring the IPFIX Information Element definition in line with the current definition of the TCP Flags header field, it is necessary to revise this definition.

The revised definition of the Information Element in [Section 3](#) was developed and approved through the IE-DOCTORS process [\[RFC7013\]](#) in August 2013. [Section 5.1 of \[RFC7013\]](#) states "This process should not in any way be construed as allowing the IE-DOCTORS to overrule IETF consensus. Specifically, Information Elements in the IANA Information Element registry which were added with IETF consensus require IETF consensus for revision or deprecation". Since the tcpControlBits Information Element was originally defined in [\[RFC5102\]](#), an IETF Proposed Standard, any revision of this Information Element definition requires IETF Consensus. The publication of this document fulfills that requirement.

The following section defines the revised tcpControlBits Information Element as in [Section 9.1 of \[RFC7013\]](#).

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 [\[RFC2119\]](#).

3. The tcpControlBits Information Element

ElementId: 6

Data Type: unsigned16

Data Type Semantics: flags

Description: TCP control bits observed for the packets of this Flow. This information is encoded as a bit field; for each TCP control bit, there is a bit in this set. The 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.

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

MSb												LSb			
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
+---+---+---+---+				+---+---+---+---+				+---+---+---+---+				+---+---+---+---+			
									N	C	E	U	A	P	R
									S	W	C	R	C	S	S
									R	E	G	K	H	T	N
+---+---+---+---+				+---+---+---+---+				+---+---+---+---+				+---+---+---+---+			

bit flag

value 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 four 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 three 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.

If exported as a single octet with reduced size encoding, this Information Element covers the low-order octet of this field (i.e., bits 0x80 to 0x01), omitting the ECN Nonce Sum and the three

Future Use bits. A collector receiving this Information Element with reduced size encoding must not assume anything about the content of these four bits.

Exporting Processes exporting this Information Element on behalf of a Metering Process that is not capable of observing any of the ECN Nonce Sum or Future Use bits 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 the CWR and ECE bits 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.

References: [[RFC0793](#)][RFC3168][[RFC3540](#)]

Revision: 1

4. IANA Considerations

IANA has updated the definition of the tcpControlBits Information Element in the the IANA IPFIX Information Element Registry [[IANA-IPFIX](#)] to reflect the changes in [Section 3](#) above, setting the revision to 1 as noted, and the revision date to the date of publication of this document.

5. Security and Privacy Considerations

This document changes the data type (and therefore the native size) of the tcpControlBits Information Element, from unsigned8 (1 octet) to unsigned16 (2 octets). As Exporting and Collecting Processes use the Information Element Length field in Templates and Options Templates and specifications for reduced size encoding where appropriate, as opposed to abstract data type sizes, for encoding and decoding Data Records, it is not expected that this will have any impact on buffer sizing during encoding and decoding. Otherwise, note that the security considerations for IPFIX [[RFC7011](#)] apply.

6. Acknowledgments

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.

7. References

7.1. Normative References

- [RFC0793] Postel, J., "Transmission Control Protocol", STD 7, [RFC 793](#), September 1981.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", [RFC 3168](#), September 2001.
- [RFC3540] Spring, N., Wetherall, D., and D. Ely, "Robust Explicit Congestion Notification (ECN) Signaling with Nonces", [RFC 3540](#), June 2003.
- [RFC7011] Claise, B., Trammell, B., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, [RFC 7011](#), September 2013.
- [RFC7013] Trammell, B. and B. Claise, "Guidelines for Authors and Reviewers of IP Flow Information Export (IPFIX) Information Elements", [BCP 184](#), [RFC 7013](#), September 2013.

7.2. Informative References

- [RFC5102] Quittek, J., Bryant, S., Claise, B., Aitken, P., and J. Meyer, "Information Model for IP Flow Information Export", [RFC 5102](#), January 2008.
- [IANA-IPFIX]
Internet Assigned Numbers Authority, , "IP Flow Information Export Information Elements (<http://www.iana.org/assignments/ipfix>)", .

Authors' Addresses

Brian Trammell
Swiss Federal Institute of Technology Zurich
Gloriastrasse 35
8092 Zurich
Switzerland

Phone: +41 44 632 70 13
Email: trammell@tik.ee.ethz.ch

Paul Aitken
Cisco Systems, Inc.
96 Commercial Quay
Commercial Street, Edinburgh EH6 6LX
United Kingdom

Phone: +44 131 561 3616
Email: paitken@cisco.com