

# An Update to the tcpControlBits IPFIX Information Element

[draft-boucadair-opsawg-rfc7125-update](#)

IETF#115

November 2022

M. Boucadair (Orange)

# The Issues

- Issue #1: RFC 7125 *deviates from the authoritative "TCP Header Flags" registry* (RFC 9293)
  - The tcpControlBits IPFIX Information Element was first defined in RFC 5102
    - RFC 5102 mirrors the TCP flags as defined in RFC 793
    - However, new control bits were defined since RFC 793
  - Then, RFC 7125 was edited with the goal to fix that ...
    - However, 7125 is also *problematic for interoperability* because, e.g., some values were deprecated since 7125 was published, e.g., removing the NS (Nonce Sum) bit as per RFC 8311
- Issue #2: Observed vs. Exported
  - The setting of control bits may be misused in some flows (e.g., attacks), calling out specific behavior for reserved bits is thus problematic

# The Proposed Fixes

- This document *removes stale* information from the IPFIX registry and *avoids future conflicts with the authoritative TCP registry*
  - ***No specific TCP flag sub-registry under IPFIX***, anymore
  - ***RFCs are not used anymore*** in the definition of the IE to point to where to find the meaning of flag bits
- Update the behavior of the exporter to avoid calling specific flag bits
  - An exporter MUST report ***all observed control bits even if no meaning is currently associated with a given control bit***

# Why an RFC is Needed

- ...Especially that the policy for the IPFIX registry is Expert Review
- But RFC 7013 says:

*“This process **should not in any way be construed as allowing the IE-DOCTORS to overrule IETF consensus**. Specifically, Information Elements in the IANA IE registry that **were added with IETF consensus require IETF consensus for revision or deprecation.**”*

# What's Next?

- Is this a problem to be solved?
- If so, how to proceed?
  - Which Stream?
    - RFC 7125 was published as an AD-sponsored document
    - However, and given the other active IPFIX-related work, request to consider adopting this draft in OPSAWG
  - Which Track?
    - RFC7125 was published as Informational (motivated by the IPFIX registry policy, if I'm not mistaken). Should the document be published in the same track or change the track (my favorite)?
  - Update (current draft) vs. bis?
- Questions and comments