

INTERNET-DRAFT
Intended Status: Informational
Expires: September 14, 2017

C. Zhou
H. Zheng
Huawei
March 13, 2017

**IP Flow Information Export (IPFIX) Information Elements Extension
for Flow Variance Information
draft-zhou-ipfix-variance-00**

Abstract

This document proposes several new Information Elements for the IP Flow Information Export (IPFIX) protocol, which are used to export variance information about the flow, regarding the sizes of the packets sampled. This kind of information is helpful to form a statistical view of the flow.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/1id-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

Copyright and License Notice

Copyright (c) 2017 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.

Table of Contents

1	Introduction	3
1.1	Terminology	3
2	Information Elements	3
3	Security Considerations	4
4	IANA Considerations	4
5	References	4
5.1	Normative References	4
5.2	Informative References	4
	Authors' Addresses	5

1 Introduction

The current set of IP Flow Information Export (IPFIX) Information Elements [[IANA-IPFIX](#)] is extensive. However, it contains no means to export information about the average size of packets in a flow, as well as the variance of the pack sizes. Having those information not only helps gain more insight of the flow from a statistical view, but also facilitates the detection of any anomaly traffic.

Below are the new Information Elements being introduced:

- o ipTotalLengthSampleMean
- o ipTotalLengthSampleVariance

The definitions of the Information Elements are given in [Section 2](#). Another reason to add these Information Elements is that it may not be practical to export every sampled packet's size and then calculate the mean and variance offline. For the sake of saving the data size to export, it is better to calculate mean and variance at the Observation Point and export only the calculated values. Algorithms such as [[RunningVariance](#)] exist to calculate mean and variance online, in a single pass, without having to save sizes of the sampled packets.

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

This document also makes use of the same terminology and definitions as [Section 2 of \[RFC5470\]](#).

2 Information Elements

Following the guidelines provided by [[RFC 7013](#)], the definitions of the new Information Elements are given below:

Name: ipTotalLengthSampleMean

Description:

The calculated mean of the ipTotalLength values of the sampled packets in a flow.

Abstract Data Type: unsigned64

ElementId: TBD

Status: current

Units: octets

Reference:

See [RFC 5102](#) for the definition of `ipTotalLength`.

Name: `ipTotalLengthSampleVariance`

The calculated variance of the `ipTotalLength` values of the sampled packets in a flow.

The result of the calculation should be converted to unsigned64.

If the result is too large to be contained in an unsigned64, then 0xFFFFFFFFFFFFFFFF should be set as the value instead.

Description:

Abstract Data Type: unsigned64

ElementId: TBD

Status: current

Reference:

See [RFC 5102](#) for the definition of `ipTotalLength`.

[3](#) Security Considerations

For this extension to the IPFIX protocol, the same security considerations as for the IPFIX protocol apply [[RFC7011](#)].

[4](#) IANA Considerations

The Information Elements defined [Section 2](#) are expected to be added to the IANA's IPFIX registry [[IANA-IPFIX](#)]. The 'TBD' values of the ElementIds should be replaced by IANA for assigned numbers.

[5](#) References

[5.1](#) Normative References

- [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.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 5226](#), May 2008.
- [RFC5470] Sadasivan, G., Brownlee, N., Claise, B., and J. Quittek, "Architecture for IP Flow Information Export", [RFC 5470](#), March 2009.

[5.2](#) Informative References

[IANA-IPFIX]

IANA, "IP Flow Information Export (IPFIX) Entities",
<<http://www.iana.org/assignments/ipfix>>.

[RunningVariance]

John D. Cook, Accurately computing running variance
<https://www.johndcook.com/blog/standard_deviation/>.

Authors' Addresses

Chong Zhou

Huawei

156 Beiqing Road, M06 Shichuang Technology Demonstration Park

Haidian, Beijing 100094

China

Email: mr.zhouchong@huawei.com

Hui Zheng (Marvin)

Huawei

101 Ruanjian Avenue, Nanjing, China

EMail: marvin.zhenghui@huawei.com

