Reporting Unobserved Fields in IPFIX

draft-aitken-ipfix-unobserved-fields-00

Paul Aitken

83rd IETF Meeting, Paris, 2012

What are “unobserved” fields?

- Some fields are not always present in all traffic.

  - eg, ICMP type and code.

- Some fields are mutually exclusive.

  - eg, IPv4 / IPv6 address, UDP / TCP port numbers.

- Some fields may be time or traffic dependent.

  - eg, end-to-end delay, server response time, traffic jitter.

Problem

- The IPFIX protocol is designed to export information about observations.
- The protocol lacks a method for reporting that requested measurements are unavailable or not applicable.
- How can we report unobserved fields?
- This document discusses several methods for reporting when fields are unavailable, reviews the advantages and disadvantage of each, and recommends which methods should be used.

Potential Solutions

- Zero-valued counters
- Multiple Templates
- CommonProperties
- Default Values
  - Default of Zero
  - Default of all-ones
  - Field-specific default values

- "Observed Fields" Bitfield
- Length of Zero
- Size field
- Structure data lists
  - Status list
  - Observed field list
  - Combined field and status list

Next Steps

- Already received some good feedback.

  -01 coming soon.

  -Export on the start of a flow "we're starting to monitor <this flow> but we don't have any data to export yet".

- Aim is standards-track extension to RFC5101(bis).

Reporting Unobserved Fields in IPFIX

draft-aitken-ipfix-unobserved-fields-00

Paul Aitken

83rd IETF Meeting, Paris, 2012