IPFIX: Architecture

draft-ietf-ipfix-architecture-03.txt

Nevil Brownlee, CAIDA | U Auckland

IPFIX Documents: Overview

- Applicability Statement
  - explains what IPFIX is, and what it's useful for
  - says what's in the other three documents
- Architecture
  - describes the IPFIX flow export system, giving detail of its components, and how they interact
- Protocol
  - describes IPFIX message formats
  - explains how the messages are carried between exporter and collector
- Information Model
  - defines information elements, i.e. what fields may appear in flow records and option data records

Editorial Changes

- Lots of editorial changes, mostly to make the draft
  - clearer
  - easier to read and understand
- Sections renumbered
  - makes the draft structure more obvious
- Some new text added to some definitions
  - *check that changes don't alter meaning!*
- Changes are summarised in opening section of the draft
- *Need to add list of issues*

Technical Changes (1)

- MUST vs SHOULD:
  - some SHOULDs change to MUST
  - architecture is an INFO draft, *use must, should, may*
- Flow Aggregates:
  - Are an optional part of the Flow Recording Process.
  - Exporting process would need to send them to Collector
  - *Do we really need aggregates?*
    Suggest removing them to simplify architecture
- Packet Selection functions:
  - Rewritten to explain them better

Technical Changes (2)

- Selective Export:
  - deleted, reduces complexity
- Flow Expiration:
  - added comment; zero inactivity timeout $\Rightarrow$ exports flow as a sequence of single-packet flows

Architecture Issues (1)

- ARCH-01:
  - Use *field* instead of *information element*
- ARCH-02:
  - Exporter not in terminology section
  - *Add Exporter,* then we'll have Exporter, Collector, Device
- ARCH-03:
  - Not clear how Options Template and Options Data should be used. *Add text to explain:*
    - data templates specify flow records
    - option templates specify options data records
    - options data fields hold information which does *not* refer to specific flows, e.g. config data or statistics

Architecture Issues (2)

- ARCH-04:
  - Make sure Terminolgy definitions are consistent with protocol (and requirememts) drafts
- ARCH-05:
  - Change IP addresses in *Flows* examples to use “documentation prefixes,” as per RFC 3330
- ARCH-06:
  - Flow aggregates. *Remove text, remove Flow Recording Process from ‘reference model’ diagram*
- ARCH-07:
  - No ‘Collecting Process’ section. *Add as section 7.5, move relevant text from sections 7.1 and 9.2*

Architecture Issues (3)

- ARCH-08:
  - No *Information Model Overview* section. Add one
  - Info Model defines fields for flow records and option data records
  - Protocol document describes how fields are encoded in IPFIX messages
  - Other systems – e.g. PSAMP – may add data or options fields; need to decide on ranges of element ids for each protocol
- ARCH-09:
  - IPFIX System Overview section needs rewriting

Architecture Issues (4)

- ARCH-10:
  - No mention of transport protocols
  - Need to say *IPFIX designed to be indeoendent of transport, see protocol document for advantages/costs of various protocols*
- ARCH-11:
  - Still need text for IANA Considerations section
  - Nevil & Benoit will write some, including ranges for IPFIX, PSAMP, etc.
  - *Suggest IPFIX chairs & document editors review requests for new field ID numbers*

Architecture Issues (4)

- ARCH-12:
  - Security Considerations. Can anyone offer more/better text for this section?

What next?

- Nevil will make edits, publish architecture-04
- Discuss on list, aim to start WG last call *before* DC IETF