

IPFIX: Architecture 04

`draft-ietf-ipfix-architecture-04.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
- Some sections restructured to improve document structure
 - parts of 'Overview of IPFIX system' section moved into 'IPFIX Protocol Details'
 - other parts of 'Overview of IPFIX System' section moved into 'IPFIX Functional and Logical Blocks'
 - added 'Information Model Overview' subsection in 'Overview of the IPFIX Protocol'

Technical Changes (1)

- Reduce confusion between 'information element' and 'field'
 - use 'field' when it referring to an element's field within a packet
 - use 'information element' everywhere else
- Add 'Exporter' to terminology section
 - now we have *Exporter*, *Collector*, *Device*
- *Terminology*: definitions improved
 - *IPFIX Protocol* draft has the normative definitions
 - definitions here may be slightly simpler

Technical Changes (2)

- Change IP addresses in 'Flows' examples to use *documentation prefixes*, as per RFC 3330
 - now using 198.18/15, network interconnect testing
- Flow aggregates
 - removed text
 - removed 'Flow Recording Process' from 'reference model' diagram
- Added 'Collecting Process' section
 - used relevant text from sections 7.1 and 9.2
- Rewrote 'IPFIX System Overview' section

Technical Changes (3)

- There was no mention of transport protocols!
 - added statement that *IPFIX is designed to be independent of transport*
 - and *See the IPFIX Protocol document for advantages/costs of various protocols*
- Added text for 'IANA Considerations' section
 - need assigned numbers for *IPFIX Version Number* and *IPFIX Template Number*; see the *Protocol* document
 - need assigned numbers for each of the *IPFIX information element Field Types*; see the *Information Model* document

Open Issues

- ARCH-03: Do we need more detail on how Options Template and Options Data should be used?
For example, add text to explain that
 - data templates specify flow records,
 - option templates specify options data records, and
 - options data fields hold information which does not refer to specific flows, e.g. config data or statistics
- ARCH-12:
 - Security Considerations. Can anyone offer more/better text for this section?

What next?

- *We need more people – especially some who haven't been working within the IPFIX WG – to read the IPFIX drafts and comment!*
- If no-one can offer more/better text for issues -03 and -12, they can probably be forgotten
- Nevil will make edits to include whatever changes arise from (and after) IETF-61, and will publish architecture-04 ASAP
- WG Chairs should then start (two-week) WG Last Call