Export of Application Information in IPFIX

IETF-79 November 10th, 2010

<draft-claise-export-application-info-in-ipfix-00.txt>

N. Ben Dvora, P. Aitken, B. Claise

How to encode the Application id?

- IANA L3 is easy -> can refer to the IANA registry
- IANA L4 is easy -> can refer to the IANA registry
- What about IANA L7?
  - No IANA registry
  - Can we have one? No because some reverse engineering is sometimes required
    - Which implies that we post the signature along with the entry
    - Which implies a common language for protocol signature

    Neither of the two will happen
  - Conclusion: we need a way to export the app id without a signature
- What about L2?
  - Not everything is etherType based. So same issue

Export of Application Information in IPFIX

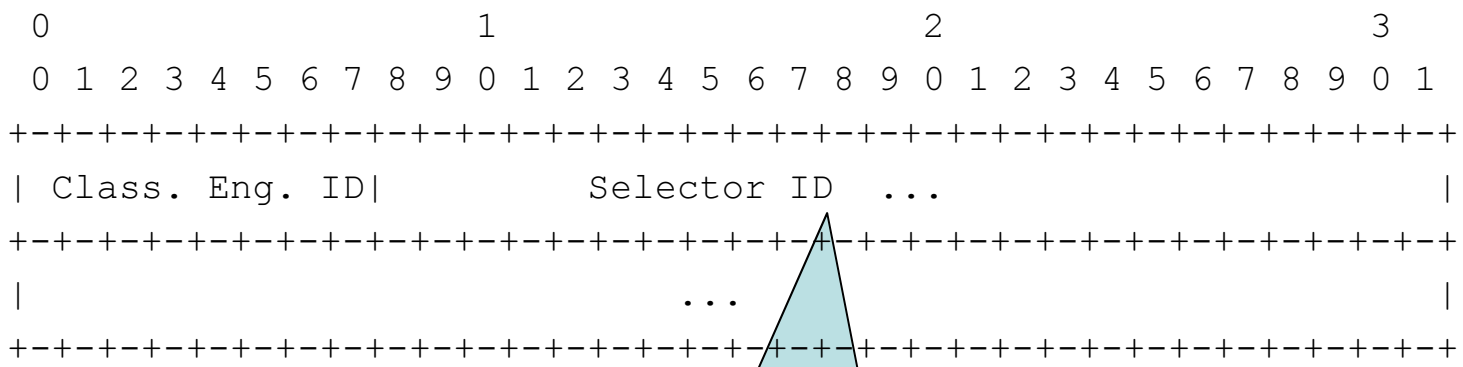


Figure 1: applicationTag Information Element

"Registry":
IANA-L3
IANA-L4
CANA-L7
CANA-L2

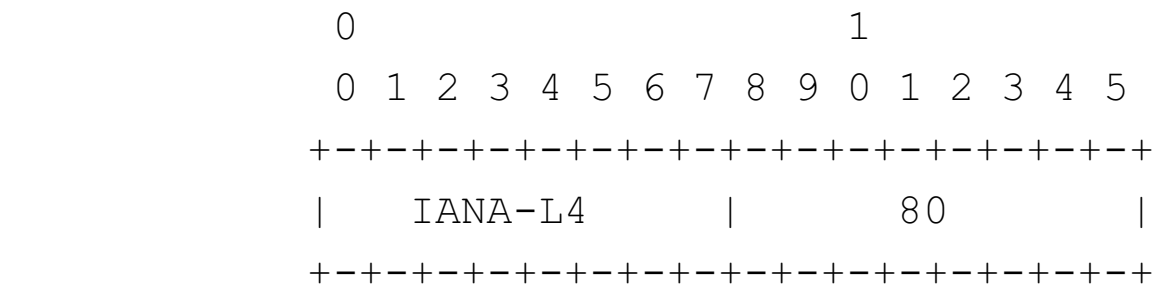
Registry:
IANA-L3 -> protocol
IANA-L4 -> port
CANA-L7 -> have to assign one per app
CANA-L2 -> have to assign one per app

CANA: Cisco Assigned Number Authority

Export of Application Information in IPFIX

- Cisco Systems way of exporting the app id
- Running code
- So an independent submission
  - Would like to get feedback anyway
- With CANA-L2 and CANA-L7 registries posted on www.cisco.com
- 3 new Information Elements:
  - applicationDescription , 94
  - applicationTag, 95
  - applicationName, 96

Export of Application Information in IPFIX



- This is HTTP, regardless of the port it runs on: 80, 8080 or 23
- If you want to know the protocol/port, export the protocol and destinationTransportPort Information Elements

Export of Application Information in IPFIX

- An Options Template Record to export the mapping
  - applicationTag, (applicationName, applicationDescription)
- Resolving IANA L4 port collisions
  - 10 different entries in IANA-L4 for UDP versus TCP
  - we define that the L4 application is always TCP related, by convention. So, whenever the collector has a conflict in looking up IANA, it would choose the TCP choice.
  - Then the 10 UDP collisions would be defined in CANA-L7

Export of Application Information in IPFIX

IETF-79 November 10th, 2010

<draft-claise-export-application-info-in-ipfix-00.txt>

N. Ben Dvora, P. Aitken, B. Claise