Export of Application Information in IPFIX

IETF-82, Nov 2011

<draft-claise-export-application-info-in-ipfix-03.txt>

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

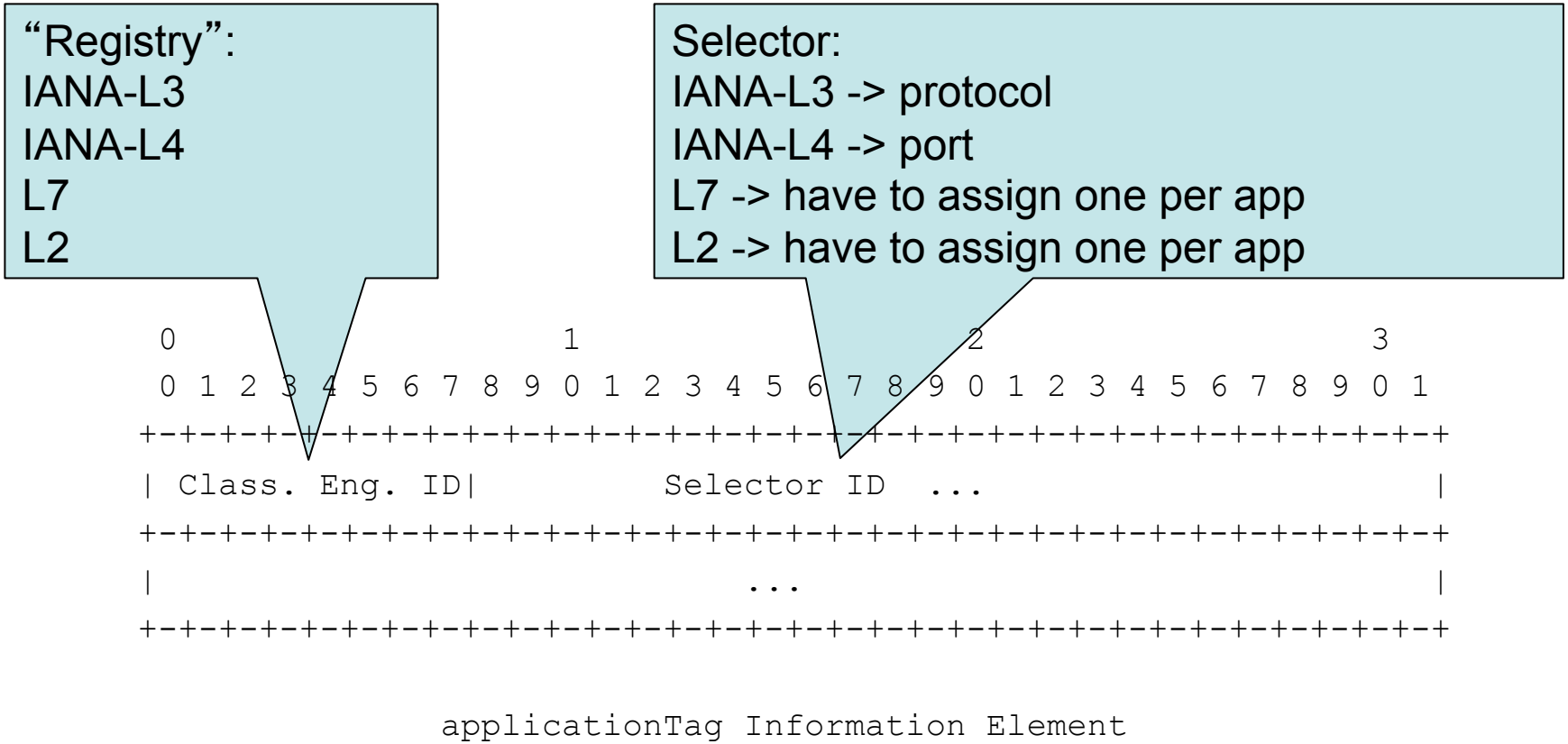
.

Application Information

- Application information is required
- What about Application Data Modeling?
  - 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 application without a signature
  - What about L2?
    - Not everything is etherType based. So same issue

Export of Application Tag in IPFIX

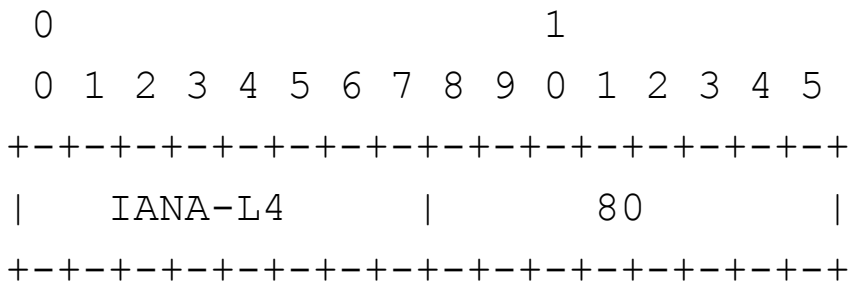


- Encoded as a variable length

Export of Application Information in IPFIX

- Informational RFC
  - With CANA-L2 and CANA-L7 registries posted on www.cisco.com
  - Note: CANA = Cisco Assigned Number Authority
- Advantages:
  - Report the application, not the destination port because port 80 might not be HTTP
  - Report the IANA-l3, IANA-L4 consistently across the industry
- 3 new Information Elements:
  - applicationDescription, 94
  - applicationTag, 95
  - applicationName, 96

Export of Application Information in IPFIX



- This I.E. value represents the HTTP application, regardless of the port it runs on: 80, 8080 or 23
- If you want to know the protocol/port, must export the protocol and destinationTransportPort Information Elements

Export of Application Information in IPFIX

- An Options Template Record to export the mapping
  - SCOPE: applicationTag,
  - NON-SCOPE: applicationName, applicationDescription
- Resolving IANA L4 port collisions
  - 10 different entries in IANA-L4 for UDP versus TCP. Some more between TCP and SCTP
  - 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 UDP and SCTP collisions would be defined in CANA-L7

New: Grouping the Applications with the 6 new attributes IEs:

- ApplicationCategoryName ,

email, newsgroup, location based services, instant-messaging, …

- ApplicationSubCategoryName ,

routing-protocol, terminal, voice-video-chat-collaboration, p2p-file-transfer, …

- ApplicationGroupName ,

example “ftp-group” contains ftp-data (port 20), ftp (port 20), ni-ftp (port 47), sftp (port 115), bftp (port 152), ftp-agent(port 574), ftps-data (port 989)

- p2pTechnology (yes, no, unassigned),
- encryptedTechnology (yes, no, unassigned),
- tunnelTechnology (yes, no, unassigned)

- Note: an Options Template Record with this information

Notes

- The IEs have been assigned already in IANA or the range <128
- Already implemented by Cisco and some collectors
- DPI vendor feedback:
  - Two vendors on the IPFIX mailing list
- ITU-T:
  - SG13/Q17 (Future Neworks: Packet forwarding and deep packet inspection for multiple services in packet-based networks and NGN environment) standardizes DPI
  - Refers to IPFIX and this application encoding
- Chris Inacio might be hosting the application id assignments, as an attempt the get an industry consensus

Feedback Received

- Could divide the L2 registry into specific registries
  - Ethertype: http://www.iana.org/assignments/ethernet-numbers
  - 802.1 16 functional address (for example, for LLDP). Note: there is no 1:1 mapping between ethertype and functional adresss
  - Everything else
- Note: an editorial mistake removed the Sub-Category. Inserted back in the newly posted version.

Conclusions

- Standardizing the app id format is important for the industry, even if we can't assign all applications in existing registries (ex: IANA)
- Then, asking for AD sponsor support to publish this draft as Informational RFC