Export of Application Information in IPFIX

IETF-80, March 2011

<draft-claise-export-application-info-in-ipfix-01.txt>

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

Application id Data Modelling?

- 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 Tag in IPFIX

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Class. Eng. ID|         Selector ID  ...                      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                              ...                              |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

                  applicationTag Information Element
```

“Registry”:
IANA-L3
IANA-L4
CANA-L7
CANA-L2

Selector:
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 way of exporting the app id (shipping code)
  - So an independent submission
  - With CANA-L2 and CANA-L7 registries posted on www.cisco.com
- 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

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   IANA-L4     |      80       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- 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
  - 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

What’s New in Version 01?

- How to handle the discrepancies between the TCP and SCTP well known ports
  - Similar to UDP/TCP discrepancies
- Grouping the Applications with the Attributes
  - 6 new IEs: category, sub-category, group, p2pTechnology, encryptedTechnology, and tunnelTechnology
  - Application assignments posted on www.cisco.com
- The introduction of an Options Template Record for the Attribute Values
  - SCOPE: applicationTag,
  - NON-SCOPE: applicationCategoryName, applicationSubCategoryName, applicationGroupName, p2pTechnology, tunnelTechnology, encryptedTechnology

What’s Next?

- Even if an individual submission, seeking for feedback
  - Implemented by some collectors
  - Received some from the ITU-T (SG13/Q17)
  - Discussed at the IPFIX Interop with one exporter vendor

Export of Application Information in IPFIX

IETF-80, March 2011

<draft-claise-export-application-info-in-ipfix-01.txt>

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