**IPFIX Guide**

Stephen Blystone

Document Version 1.0

Last Updated: Mar 25, 2018

Table of Contents

[**Revision History** 3](#_Toc510207693)

[**IPFIX Definitions** 3](#_Toc510207694)

[**Configuring IPFIX on Open vSwitch** 5](#_Toc510207695)

[**References** 5](#_Toc510207696)

# **Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Changes** |
| 1.0 | 3/25/2018 | Initial Version |

# **IPFIX Definitions**

1. <https://tools.ietf.org/html/rfc7011>
2. **Observation Domain** is the largest set of Observation Points for which Flow information can be aggregated by a metering process.
   1. **NOTE: It is recommended that Observation Domain IDs be unique per IPFIX Device.**
3. **Observation Point** is location in network where packets can be observed.
   1. NOTE: That every Observation Point is associated with an Observation Domain. One Observation Point may be a superset of several other Observation Points.
4. **Packet Treatment** are actions performed on a packet by a forwarding device.
   1. Includes forwarding, dropping, delaying for traffic-shaping purposes, etc.
5. **Traffic Flow** is set of packets passing an Observation Point during a certain time interval.
   1. All packets belonging to particular flow have common set of properties. Each property is defined as the result of applying a function to the values of:
      1. One or more packet header fields (e.g. destination IP address), transport header fields (e.g. destination port number), or application header fields (e.g. RTP header fields).
      2. One or more characteristics of the packet itself (e.g. number of MPLS labels, etc.)
      3. One or more of the fields derived from Packet Treatment (e.g. next-hop IP address, the output interface, etc.)
6. **Flow Key**
   1. Flow Key is the fields that define a Flow (i.e. properties common to all packets in the Flow) and the fields that:
      1. Belong to the packet header (e.g. destination IP address), OR
      2. Are a property of the packet itself (e.g. packet length), OR
      3. Are derived from Packet Treatment (e.g. Autonomous System number)
   2. The traditional ‘5-tuple’ Flow Key of source and destination IP address, source and destination transport port, and transport protocol groups together all packets belonging to a single direction of communication on a single socket.
7. **Flow Record** contains information about a specific Flow that was observed at an Observation Point.
   1. Measures properties of the Flow (e.g. the total number of bytes for all the Flow’s packets) and usually contains characteristic properties of the Flow (e.g. source IP address).
8. **Metering Process** generates Flow Records.
   1. Inputs to the process are packet headers, characteristics, and Packet Treatment observed at one or more Observation Points.
   2. Consists of a set of functions that include packet header capturing, timestamping, sampling, classifying, and maintaining Flow Records.
   3. The maintenance of Flow Records may include creating new records, updating existing ones, computing Flow statistics, deriving further Flow properties, detecting Flow expiration, passing Flow Records to the Exporting Process, and deleting Flow Records.
9. **Exporting Process** sends IPFIX messages to one or more Collecting Processes. The Flow Records in the Messages are generated by one or more Metering Processes.
10. **Exporter** is the device that hosts one or more Exporting Processes.
11. **IPFIX Device** hosts at least one Exporting Process. It may host further Exporting Processes as well as arbitrary numbers of Observation Points and Metering Processes.
12. **Collecting Process** receives IPFIX Messages from one or more Exporting Processes.
    1. Might process or store Flow Records received within these messages
13. **Collector** is device that hosts one or more Collecting Processes.
14. **Template** is an ordered sequence of <type, length> pairs used to completely specify the structure and semantics of a particular set of information that needs to be communicated from an IPFIX Device to a Collector.
    1. Each Template is uniquely identifiable by means of a Template ID
15. **IPFIX Message** is a message that originates at the Exporting Process and carries the IPFIX records of this Exporting Process, and whose destination is a Collecting Process.
    1. IPFIX Message is encapsulated at the transport layer.
16. **Message Header** is the first part of the IPFIX Message.
    1. Contains IPFIX version, length of the message, message sequence number, etc.
17. **Template Record** defines the structure and interpretation of fields in a Data Record.
18. **Data Record** is a record that contains values of the parameters corresponding to a Template Record.
19. **Options Template Record** is a Template Record that defines the structure and interpretation of fields in a Data Record, including defining how to scope the applicability of the Data Record.
20. **Set** is collection of records that have similar structure, prefixed by a header.
    1. Zero or more Sets follow the IPFIX Message Header
    2. There are: Template Sets, Options Template Sets, and Data Sets
21. **Template Set** is a collection of one or more Template Records that have been grouped together in an IPFIX Message.
22. **Options Template Set** is collection of one or more Options Template Records that have been grouped together in an IPFIX Message.
23. **Data Set** is one or more Data Records, of the same time, that are grouped together in an IPFIX Message.
24. **Information Element** is a protocol- and encoding-independent description of an attribute that may appear in an IPFIX Record.
    1. <https://www.iana.org/assignments/ipfix/ipfix.xhtml>

# **Configuring IPFIX on Open vSwitch**

1. <https://splash.riverbed.com/docs/DOC-5783>
2. <http://www.openvswitch.org/support/dist-docs/ovs-vsctl.8.txt>
3. Launch mininet
4. In another terminal window, run the following command. The highlighted parameters may change based on your VM’s values:

sudo ovs-vsctl set bridge s1 ipfix=@i -- --id=@i create IPFIX targets=\”10.28.34.16:4739\” obs\_domain\_id=123 obs\_point\_id=456 cache\_active\_timeout=60 cache\_max\_flows=13 sampling=20 other\_config:enable-input-sampling=false other\_config:enable-tunnel-sampling=false

s1 = Open vSwitch to apply to.

10.28.34.16 = IP address of IPFIX collector.

4739 = Port of IPFIX collector.

123 = Observation Domain ID. **Each Open vSwitch needs a different Observation Domain ID**

456 = Observation Point ID.

other\_config:enable-input-sampling = TODO: What is this?

other\_config:enable-tunnel-sampling = TODO: What is this?

1. To view the changes, run “ovs-vsctl list bridge” and you should see letters and numbers next to “ipfix”. If you see “[]” then it was not successful.

# **Remove IPFIX from Open vSwitch**

1. If you need to remove IPFIX from an Open vSwitch:

sudo ovs-vsctl clear bridge s1 ipfix

# **References**

1. IPFIX Information Elements

<https://www.iana.org/assignments/ipfix/ipfix.xhtml>

1. IPFIX RFC

<https://tools.ietf.org/html/rfc7011>

1. Parameters that the version of Open vSwitch that comes with Mininet can configure

<http://www.openvswitch.org/support/dist-docs-2.5/ovs-vswitchd.conf.db.5.pdf>

<https://www.mail-archive.com/dev@openvswitch.org/msg60447.html>

<https://mail.openvswitch.org/pipermail/ovs-dev/2016-June/315581.html>