IPFIX working group
Internet Draft
draft-aitken-ipfix-new-infos-03
Intended Status: Proposed Standard
Expires: September 17, 2008

Editor P. Aitken
Editor B. Claise
Cisco Systems, Inc.
March 17, 2008

New Information Elements from the IPFIX Information Model

Status of this Memo

Copyright Notice

Abstract

This document specifies the IPFIX protocol that serves for transmitting IP traffic flow information over the network. In order

to transmit IP traffic flow information from an exporting process to an information collecting process, a common representation of flow data and a standard means of communicating them is required. This document describes how the IPFIX data and templates records are carried over a number of transport protocols from an IPFIX exporting process to an IPFIX collecting process.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Table of Contents

1. Introduction

The IPFIX Information Model [RFC5102] defines an extensible list of Information Elements which may be transmitted by the IPFIX protocol [RFC5101].

This document lists a series of new Information Elements to update the IPFIX Information Model, and acts as the persistent publication medium requested in the IANA considerations section of the IPFIX Information Model [RFC5102] ("The specification of new IPFIX Information Elements MUST use the template specified in section 2.1 and MUST be published using a well established and persistent publication medium").

2. Terminology

IPFIX-specific terminology used in this document is defined in section 2 of the IPFIX Protocol [RFC5101]. As in the IPFIX Protocol [RFC5101], these IPFIX-specific terms have the first letter of a word capitalized when used in this document.

2.1 IPFIX Documents Overview

The IPFIX Protocol [RFC5101] provides network administrators with access to IP flow information.

The architecture for the export of measured IP flow information out of an IPFIX exporting process to a collecting process is defined in the IPFIX Architecture [IPFIX-ARCH], per the requirements defined in RFC 3917 [RFC3917].

The IPFIX Architecture [IPFIX-ARCH] specifies how IPFIX Data Records and Templates are carried via a congestion-aware transport protocol from IPFIX Exporting Processes to IPFIX Collecting Processes.

IPFIX has a formal description of IPFIX Information Elements, their name, type and additional semantic information, as specified in the IPFIX Information Model [RFC5102].

Finally the IPFIX Applicability Statement [IPFIX-AS] describes what type of applications can use the IPFIX protocol and how they can use the information provided. It furthermore shows how the IPFIX framework relates to other architectures and frameworks.

2.2 PSAMP Documents Overview

The document "A Framework for Packet Selection and Reporting" [PSAMP-FMWK], describes the PSAMP framework for network elements to select subsets of packets by statistical and other methods, and to export a stream of reports on the selected packets to a collector.

The set of packet selection techniques (sampling, filtering, and hashing) supported by PSAMP are described in "Sampling and Filtering Techniques for IP Packet Selection" [PSAMP-TECH].

The PSAMP protocol [PSAMP-PROTO] specifies the export of packet information from a PSAMP Exporting Process to a PSAMP Collecting Process. Like IPFIX, PSAMP has a formal description of its information elements, their name, type and additional semantic information. The PSAMP information model is defined in [PSAMP-INFO].

Finally [PSAMP-MIB] describes the PSAMP Management Information Base.

3. Information Element Identifiers

The value of the Information Element identifiers are in the range of 1 - 32767. Within this range, Information Element identifier values in the sub-range of 1-127 are compatible with field types used by NetFlow version 9 [RFC3954].

The following list gives an overview of the new Information Element identifiers that are in the range 1-127. These Information Elements were previously RESERVED according to the IPFIX Information Model [RFC5102] and IANA.

ID	Name
82	interfaceName
83	interfaceDescription
~	~
89	forwardingStatus
~	~
91	mplsTopLabelPrefixLength
~	~
98	postIpDiffServCodePoint
99	multicastReplicationFactor

The following list gives an overview of new Information Elements, not part of the RESERVED range. It also displays the ideal Information Element identifiers that we would like IANA to assign. Note that the following web site http://ipfix.netlab.nec.de/infoElements.php, maintained by the IPFIX Chair (Juergen Quittek) is a placeholder for the allocation of the Information Element Id, while waiting for the IANA assignments.

ID	Name
225	postNATSourceIPv4Address
226	postNATDestinationIPv4Address
227	postNAPTSourceTransportPort
228	postNAPTDestinationTransportPort
229	natOriginatingAddressRealm
230	natEvent
231	InitiatorOctets
232	ResponderOctets
233	firewallEvent
234	ingressVRFID
235	egressVRFID
236	VRFname
~	~
240	ethernetHeaderLength
241	ethernetPayloadLength
242	ethernetTotalLength
243	dot1qVlanId
244	dot1qPriority
245	dot1qCustomerVlanId
246	dot1qCustomerPriority
247	metroEvcId
248	metroEvcType
249	pseudoWireId
250	pseudoWireType
251	pseudoWireControlWord
252	ingressPhysicalInterface
253	egressPhysicalInterface
254	postDot1qVlanId
255	postDot1qCustomerVlanId
256	ethernetType
~	~
335	selectorName

4. New Information Elements in the range 1-127

4.1 interfaceName

Description:
A short name uniquely describing an interface, eg "Eth1/0".
Abstract Data Type: string
ElementId: 82
Status: current
Reference:

See RFC 2863 [RFC2863] for the definition of the ifName object.

4.2 interfaceDescription

Description:
The description of an interface, eg "FastEthernet 1/0" or "ISP connection".
Abstract Data Type: string
ElementId: 83
Status: current
Reference:
See RFC 2863 [RFC2863] for the definition of the ifDescr object.

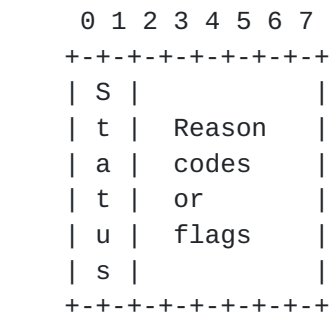
4.3 forwardingStatus

Description:
Describes the forwarding status of the flow and any attached reasons.

Forwarding Status is a variable length field with length of 1, 2 or 4 octets.

*** IANA ACTION ***

The values of this element are to be allocated from IANA registries which can be found at http://www.iana.org/assignments/...
A. When length = 1 octet:



Status:

00b = Unknown
01b = Forwarded
10b = Dropped
11b = Consumed

Reason codes:

Reason codes are defined per status code.

Reason Code (status = 01b, Forwarded):

000000b = Unknown
000001b = Fragmented
000010b = Not Fragmented

Reason Code (status = 10b, Dropped):

000000b = Unknown
000001b = ACL Deny
000010b = ACL drop
000011b = Unroutable
000100b = Adjacency
000101b = Fragmentation & DF set
000110b = Bad header checksum
000111b = Bad total Length
001000b = Bad Header Length
001001b = bad TTL
001010b = Policer
001011b = WRED
001100b = RPF
001101b = For us
001110b = Bad output interface
001111b = Hardware

Reason Code (status = 11b, Consumed):

000000b = Unknown
000001b = Punt Adjacency
000010b = Incomplete Adjacency
000011b = For us

Example 1:

```
hex dump: 01 000000
decode:   01         -> Forward
             000000  -> No further information
```

Example 2:

```
hex dump: 10 001001
decode  : 10          -> Drop
             001001   -> Fragmentation & DF set
```

B. When length = 2 octets:

A length of 2 indicates an extended reason:

```
bit 0 0 0 0 0 0 0 0  0 0 1 1 1 1 1 1
    0 1 2 3 4 5 6 7  8 9 0 1 2 3 4 5
  +----------------+----------------+
  |Status & Reason | Extended Reason|
  +----------------+----------------+
```

The status and reason are as defined in (A) above. The extended reasons are yet to be defined.

C. When length = 4 octets:

If there are further extensions to the reason, the field length is 4:

```
  0 0 0 0 0 0 0 0  0 0 1 1 1 1 1 1  1 1 1 1 2 2 2 2  2 2 2 2 2 2 3 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
+----------------+----------------+----------------+----------------+
|Status & Reason | Extended Reason|        Further Extensions       |
+----------------+----------------+----------------+----------------+
```

The status, reason and extended reason are as defined in (B) above. Further extended reasons are yet to be defined.

Abstract Data Type: octetArray
Data Type Semantics: flags
ElementId: 89
Status: current

4.4 mplsTopLabelPrefixLength

Description:
The prefix length of the subnet of the mplsTopLabelIPv4Address that the MPLS top label will cause the Flow to be forwarded to.
Abstract Data Type: unsigned 8
Data Type Semantics: identifier
ElementId: 91
Status: current
Units: bits
Range: The valid range is 0-32
Reference:
See RFC 3031 for the association between MPLS labels and prefix lengths.

4.5 postIpDiffServCodePoint

Description:
The definition of this Information Element is identical to the definition of Information Element 'ipDiffServCodePoint', except that it reports a potentially modified value caused by a middlebox function after the packet passed the Observation Point.
Abstract Data Type: unsigned8
Data Type Semantics: identifier
ElementId: 98
Status: current
Range: The valid range is 0-63.
Reference:
See RFC 3260 [RFC3260] for the definition of the Differentiated Services Field. See section 5.3.2 of RFC 1812 [RFC1812] and RFC 791 [RFC791] for the definition of the IPv4 TOS field. See RFC 2460 [RFC2460] for the definition of the IPv6 Traffic Class field. See the IPFIX Informaiton Model [RFC5102] for the 'ipDiffServCodePoint' specification.

4.6 multicastReplicationFactor

Description:
The amount of multicast replication that's applied to a traffic stream.
Abstract Data Type:
Data Type Semantics:
ElementId: 99
Status: current
Reference:
See RFC 1112 [RFC1112] for the specification of reserved IPv4 multicast addresses. See RFC 4291 [RFC4291] for the specification of reserved IPv6 multicast addresses.

5. New Information Elements in the range 128-32767

5.1 postNATSourceIPv4Address

Description:
The definition of this Information Element is identical to the definition of Information Element 'sourceIPv4Address', except that it reports a modified value caused by a NAT middlebox function after the packet passed the Observation Point.
Abstract Data Type: ipv4Address
Data Type Semantics: identifier
ElementId: 225

Status: current
Reference:
See RFC 791 [RFC791] for the definition of the IPv4 source address field. See RFC 3022 [RFC3022] for the definition of NAT. See RFC 3234 [RFC3234] for the definition of middleboxes.

5.2 postNATDestinationIPv4Address

Description:
The definition of this Information Element is identical to the definition of Information Element 'destinationIPv4Address', except that it reports a modified value caused by a NAT middlebox function after the packet passed the Observation Point.
Abstract Data Type: ipv4Address
Data Type Semantics: identifier
ElementId: 226
Status: current
Reference:
See RFC 791 [RFC791] for the definition of the IPv4 destination address field. See RFC 3022 [RFC3022] for the definition of NAT. See RFC 3234 [RFC3234] for the definition of middleboxes.

5.3 postNAPTSourceTransportPort

Description:
The definition of this Information Element is identical to the definition of Information Element 'sourceTransportPort', except that it reports a modified value caused by a Network Address Port Translation (NAPT) middlebox function after the packet passed the Observation Point.
Abstract Data Type: unsigned16
Data Type Semantics: identifier
ElementId: 227
Status: current
Reference:
See RFC 768 [RFC768] for the definition of the UDP source port field. See RFC 793 [RFC793] for the definition of the TCP source port field. See RFC 4960 [RFC4960] for the definition of SCTP.
See RFC 3022 [RFC3022] for the definition of NAPT. See RFC 3234 [RFC3234] for the definition of middleboxes.
Additional information on defined UDP and TCP port numbers can be found at http://www.iana.org/assignments/port-numbers.

5.4 postNAPTDestinationTransportPort

Description:
The definition of this Information Element is identical to the definition of Information Element 'destinationTransportPort', except that it reports a modified value caused by a Network Address Port Translation (NAPT) middlebox function after the packet passed the Observation Point.
Abstract Data Type: unsigned16
Data Type Semantics: identifier
ElementId: 228
Status: current
Reference:
See RFC 768 [RFC768] for the definition of the UDP source port field. See RFC 793 [RFC793] for the definition of the TCP source port field. See RFC 4960 [RFC4960] for the definition of SCTP. See RFC 3022 [RFC3022] for the definition of NAPT. See RFC 3234 [RFC3234] for the definition of middleboxes.
Additional information on defined UDP and TCP port numbers can be found at http://www.iana.org/assignments/port-numbers.

5.5 natOriginatingAddressRealm

Description:
Indicates whether the session was created because traffic originated in the private or public address realm. postNATSourceIPv4Address, postNATDestinationIPv4Address, postNAPTSourceTransportPort, and postNAPTDestinationTransportPort are qualified with the address realm in perspective.
The allowed values are:
Private: 1
Public: 2
Abstract Data Type: unsigned8
Data Type Semantics: flags
ElementId: 229
Status: current
Reference:
See RFC 3022 [RFC3022] for the definition of NAT.

5.6 natEvent

Description:
Indicates a NAT event. The allowed values are:
1 - Create event.
2 - Delete event.

A Create event is generated when a NAT translation is created, whether dynamically or statically. A Delete event is generated when a NAT translation is deleted.

Abstract Data Type: unsigned8
Data Type Semantics:
ElementId: 230
Status: current
Reference:
See RFC 3022 [RFC3022] for the definition of NAT.

5.7 initiatorOctets

Description:
The total number of layer 4 payload bytes in a flow from the initiator. The initiator is the device which triggered the session creation, and remains the same for the life of the session.

Abstract Data Type: unsigned64
Data Type Semantics:
ElementId: 231
Status: current

5.8 responderOctets

Description:
The total number of layer 4 payload bytes in a flow from the responder. The responder is the device which replies to the initiator, and remains the same for the life of the session.

Abstract Data Type: unsigned64
Data Type Semantics:
ElementId: 232
Status: current

5.9 firewallEvent

Description:
Indicates a firewall event. The allowed values are:

0 - Ignore (invalid)
1 - Flow Created
2 - Flow Deleted
3 - Flow Denied
4 - Flow Alert

Abstract Data Type: unsigned8
Data Type Semantics:
ElementId: 233

Status: current

5.10 ingressVRFID

Description:
An unique identifier of the VRFname where the packets of this flow are being received. This identifier is unique per Metering Process
Abstract Data Type: unsigned32
Data Type Semantics:
ElementId: 234
Status: current

5.11 egressVRFID

Description:
An unique identifier of the VRFname where the packets of this flow are being sent. This identifier is unique per Metering Process
Abstract Data Type: unsigned32
Data Type Semantics:
ElementId: 235
Status: current

5.12 VRFname

Description:
The name of a VPN Routing and Forwarding table (VRF).
Abstract Data Type: string
ElementId: 236
Status: current
Reference:
See RFC 4364 [RFC4364] for the definition of VRF.

5.13 ethernetHeaderLength

Description:
The difference between the length of an Ethernet frame (minus the FCS) and the length of its MAC Client Data section (including any padding) as defined in section 3.1 of [IEEE.802-3.2005]. It does not include the Preamble, SFD and Extension field lengths.
Abstract Data Type: unsigned8
Data Type Semantics: identifier
ElementId: 240
Status: current
Units: octets

Reference:
(1) [IEEE.802-3.2005]

5.14 ethernetPayloadLength

Description:
The length of the MAC Client Data section (including any padding) of a frame as defined in section 3.1 of [IEEE.802-3.2005].
Abstract Data Type: unsigned16
Data Type Semantics: identifier
ElementId: 241
Status: current
Units: octets
Reference:
(1) [IEEE.802-3.2005]

5.15 ethernetTotalLength

Description:
The total length of the Ethernet frame (excluding the Preamble, SFD, Extension and FCS fields) as described in section 3.1 of [IEEE.802-3.2005].
Abstract Data Type: unsigned16
Data Type Semantics: identifier
ElementId: 242
Status: current
Units: octets
Reference:
(1) [IEEE.802-3.2005]

5.16 dot1qVlanId

Description:
The value of the 12-bit VLAN Identifier portion of the Tag Control Information field of an Ethernet frame as described in section 3.5.5 of [IEEE.802-3.2005]. The structure and semantics within the Tag Control Information field are defined in IEEE P802.1Q. In case of a QinQ frame, it represents the outer tag's VLAN identifier and in case of an IEEE 802.1ad frame it represents the Service VLAN identifier in the S-TAG Tag Control Information (TCI) field as described in [IEEE.802-1ad.2005].
Abstract Data Type: unsigned16
Data Type Semantics: identifier
ElementId: 243
Status: current
Reference:
(1) [IEEE.802-3.2005]

(2) [IEEE.802-1ad.2005]

5.17 dot1qPriority

Description:
The value of the 3-bit User Priority portion of the Tag Control Information field of an Ethernet frame as described in section 3.5.5 of [IEEE.802-3.2005]. The structure and semantics within the Tag Control Information field are defined in IEEE P802.1Q. In case of a QinQ frame, it represents the outer tag's 3-bit Class of Service (CoS) identifier and in case of an IEEE 802.1ad frame it represents the 3-bit Priority Code Point (PCP) portion of the S-TAG Tag Control Information (TCI) field as described in [IEEE.802-1ad.2005].
Abstract Data Type: unsigned8
Data Type Semantics: identifier
ElementId: 244
Status: current
Reference:
(1) [IEEE.802-3.2005]
(2) [IEEE.802-1ad.2005]

5.18 dot1qCustomerVlanId

Description:
In case of a QinQ frame, it represents the inner tag's (*) VLAN identifier and in case of an IEEE 802.1ad frame it represents the Customer VLAN identifier in the C-TAG Tag Control Information (TCI) field as described in [IEEE.802-1ad.2005].
(*) Note: the 801.2Q tag directly following the outer one.
Abstract Data Type: unsigned16
Data Type Semantics: identifier
ElementId: 245
Status: current
Reference:
(1) [IEEE.802-1ad.2005]
(2) [IEEE.802-1Q.2003]

5.19 dot1qCustomerPriority

Description:
In case of a QinQ frame, it represents the inner tag's (*) Class of Service (CoS) identifier and in case of an IEEE 802.1ad frame it represents the 3-bit Priority Code Point (PCP) portion of the C-TAG Tag Control Information (TCI) field as described in [IEEE.802-1ad.2005].
(*) Note: the 801.2Q tag directly following the outer one.

Abstract Data Type: unsigned8
Data Type Semantics: identifier
ElementId: 246
Status: current
Reference:
(1) [IEEE.802-1ad.2005]
(2) [IEEE.802-1Q.2003]

5.20 metroEvcId

Description:
The EVC Service Attribute which uniquely identifies the Ethernet Virtual Connection (EVC) within a Metro Ethernet Network, as defined in section 6.2 of MEF 10.1. The MetroEVCID is encoded in a string of up to 100 characters.
Abstract Data Type: string
ElementId: 247
Status: current
Reference:
(1) MEF 10.1 (Ethernet Services Attributes Phase 2)
(2) MEF16 (Ethernet Local Management Interface)

5.21 metroEvcType

Description:
The 3-bit EVC Service Attribute which identifies the type of service provided by an EVC.
Abstract Data Type: unsigned8
Data Type Semantics: identifier
ElementId: 248
Status: current
Reference:
(1) MEF 10.1 (Ethernet Services Attributes Phase 2)
(2) MEF16 (Ethernet Local Management Interface)

5.22 pseudoWireId

Description:
A 32-bit non-zero connection identifier, which together with the pseudoWireType, identifies the Pseudo Wire (PW) as defined in RFC 4447 [RFC4447].
Abstract Data Type: unsigned32
Data Type Semantics: identifier
ElementId: 249
Status: current
Reference:
See RFC 4447 [RFC4447] for pseudowire definitions.

5.23 pseudoWireType

Description:
The value of this information element identifies the type of MPLS Pseudo Wire (PW) as defined in RFC 4446.
Abstract Data Type: unsigned16
Data Type Semantics: identifier
ElementId: 250
Status: current
Reference:
See RFC 4446 [RFC4446] for the pseudowire type definition, and http://www.iana.org/assignments/pwe3-parameters for the IANA Pseudowire Types Registry.

5.24 pseudoWireControlWord

Description:
The 32-bit Preferred Pseudo Wire (PW) MPLS Control Word as defined in Section 3 of RFC 4385 [RFC4385].
Abstract Data Type: unsigned32
Data Type Semantics: identifier
ElementId: 251
Status: current
Reference:
See RFC 4385 [RFC4385] for the Pseudo Wire Control Word definition.

5.25 ingressPhysicalInterface

Description:
The index of a networking device's physical interface (example, a switch port) where packets of this flow are being received.
Abstract Data Type: unsigned32
Data Type Semantics: identifier
ElementId: 252
Status: current
Reference:
See RFC 2863 [RFC2863] for the definition of the ifIndex object.

5.26 egressPhysicalInterface

Description:
The index of a networking device's physical interface (example, a switch port) where packets of this flow are being sent.

Abstract Data Type: unsigned32
Data Type Semantics: identifier
ElementId: 253
Status: current
Reference:
See RFC 2863 [RFC2863] for the definition of the ifIndex object.

5.27 postDot1qVlanId

Description:
The definition of this Information Element is identical to the definition of Information Element 'dot1qVlanId', except that it reports a potentially modified value caused by a middlebox function after the packet passed the Observation Point.
Abstract Data Type: unsigned16
Data Type Semantics: identifier
ElementId: 254
Status: current
Reference:
(1) [IEEE.802-3.2005]
(2) [IEEE.802-1ad.2005]

5.28 postDot1qCustomerVlanId

Description:
The definition of this Information Element is identical to the definition of Information Element 'dot1qCustomerVlanId', except that it reports a potentially modified value caused by a middlebox function after the packet passed the Observation Point.
Abstract Data Type: unsigned16
Data Type Semantics: identifier
ElementId: 255
Status: current
Reference:
(1) [IEEE.802-1ad.2005]
(2) [IEEE.802-1Q.2003]

5.29 ethernetType

Description:
The Ethernet type field of an Ethernet frame that identifies the MAC client protocol carried in the payload as defined in paragraph 1.4.349 of [IEEE.802-3.2005].
Abstract Data Type: unsigned16
Data Type Semantics: identifier
ElementId: 256
Status: current

Reference:
(1) [IEEE.802-3.2005]
(2) Ethertype registry available at
http://standards.ieee.org/regauth/ethertype/eth.txt

5.30 selectorName

Description:
The name of a selector identified by a selectorID. Globally unique per Metering Process.
Abstract Data Type: string
ElementId: 335
Status: current

6. Relationship between dot1qVlanId and vlanId

The IPFIX Information Model [RFC5102] specifies the vlanId Information Element, while this document specifies the dot1qVlanId.

The vlanId Information Element references [IEEE.802-1Q.2003], while the dot1qVlanId references [IEEE.802-3.2005] and [IEEE.802-1ad.2005]. Since the [IEEE.802-1ad.2005] supersedes the [IEEE.802-1Q.2003] (it mentions: "Amendment to IEEE Std 802.1Q-2005".), then the dot1qVlanId supersedes vlanId.

***IANA ACTION ***

As a consequence the vlanId specified in the IPFIX Information Model [RFC5102] is now deprecated:

vlanId
Description:
The IEEE 802.1Q VLAN identifier (VID) extracted from the Tag Control Information field that was attached to the IP packet.
Abstract Data Type: unsigned16
Data Type Semantics: identifier
ElementId: 58
Status: deprecated
Reference:
See [IEEE.802-1Q.2003].

***IANA ACTION ***

This document also specifies postDot1qVlanId, in connection with the dot1qCustomerVlanId. As a consequence, the postVlanId specified in the IPFIX Information Model [RFC5102] is now deprecated:

postVlanId
   Description:
      The definition of this Information Element is identical to the
      definition of Information Element 'vlanId', except that it
      reports a potentially modified value caused by a middlebox
      function after the packet passed the Observation Point.
   Abstract Data Type: unsigned16
   Data Type Semantics: identifier
   ElementId: 59
   Status: deprecated
   Reference:
      See [IEEE.802-1Q.2003].

7. Relationship between interface related Information Elements

The IPFIX Information Model [RFC5102] specifies the ingressInterface (#10) and egressInterface (#14) information elements, while this document specifies the ingressPhysicalInterface and egressPhysicalInterface.

The IPFIX definitions for ingressInterface and egressInterface are somewhat vague, essentially in case of the virtual interfaces. Let us consider traffic transiting a tunnel, where the virtual and physical interfaces are different. If one implementation uses the ingressInterface and egressInterface to report the physical interfaces while another implementation uses the same information elements to report the virtual interfaces, without somehow making this clear to the Collector, then any reports and analysis are going to be skewed.

The specifications of ingressPhysicalInterface and egressPhysicalInterface clarifies the situation.

The relationship between the multiple sub-layers of network interfaces is specified in the ifStackTable MIB table in the interface MIB [RFC2863].

8. IANA Considerations

This document specifies new IPFIX Information Elements in two ranges.

Information Elements in the range 1 to 127 are compatible with field types used by NetFlow version 9 [RFC3954]. These Information Elements were previously RESERVED according to the IPFIX Information Model [RFC5102] and IANA. These should be allocated immediately with the specified IDs to retain backwards compatibility with NetFlow version 9 [RFC3954].

The remainder of the Information Elements (in the range 128 and up) are new, and are therefore subject to expert review as specified in the IPFIX Information Model [RFC5102]. They are listed here with the ideal Information Element identifiers that we would like IANA to assign.

In addition, some IANA actions have been highlighted in section 7.

Finally, the forwardingStatus Information Element requires the creation of new IANA registries.

9. References

9.1 Normative References

[RFC768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[RFC791] J. Postel, "Internet Protocol. DARPA Internet Program. Protocol Specification," RFC 791, September 1981.

[RFC793] J. Postel, "Transmission Control Protocol", September 1981.

[RFC1112] B. Braden, "Requirements for Internet hosts - communication layers", Octobre 1989.

[RFC1812] Baker, F., Ed., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2863] McCloghrie, K. and F. Kastenholz, "The Interfaces Group MIB", RFC 2863, June 2000.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.

[RFC4385] Bryant, S., Swallow, G., Martini, L., and D. McPherson, "Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN", RFC 4385, February 2006.

[RFC4446] Martini, L., "IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)", BCP 116, RFC 4446, April 2006.

[RFC4447] Martini, L., Ed., Rosen, E., El-Aawar, N., Smith, T., and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", RFC 4447, April 2006.

[RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, September 2007.

[RFC5101] Claise, B., Ed., "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information", RFC 5101, January 2008.

[RFC5102] Quittek, J., Bryant, S., Claise, B., Aitken, P., and J. Meyer, "Information Model for IP Flow Information Export", RFC 5102, January 2008.

[IEEE.802-1ad.2005]
"IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks---Amendment 4: Provider Bridges", IEEE 802.1ad-2005, May 26, 2006.

[IEEE.802-1Q.2003]
"IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks", IEEE 802.1Q,2003 Edition-2003.

[IEEE Std 802.1Q-2005]
"IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks", IEEE 802.1Q-2005, May 19, 2006.

[IEEE.802-3.2005]
"IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications", IEEE 802.3-2005, Dec 09, 2005.

[ISO_IEC.7498-1_1994]
International Organization for Standardization, "Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Mode", ISO Standard 7498-1:1994, June 1996.

9.2 Informative References

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

[RFC3234] Carpenter, B. and S. Brim, "Middleboxes: Taxonomy and Issues", RFC 3234, February 2002.

[RFC3260] Grossman, D., "New Terminology and Clarifications for Diffserv", RFC 3260, April 2002.

[RFC3917] Quittek, J., Zseby, T., Claise, B., Zander, S., "Requirements for IP Flow Information Export" RFC 3917, October 2004

[RFC3954] Claise, B., et al "Cisco Systems NetFlow Services Export Version 9", RFC 3954, October 2004

[IPFIX-ARCH] Sadasivan, G., Brownlee, N., Claise, B., Quittek, J., "Architecture Model for IP Flow Information Export" draft-ietf-ipfix-architecture-12, September 2006

[IPFIX-AS] Zseby, T., Boschi, E., Brownlee, N., Claise, B., "IPFIX Applicability", draft-ietf-ipfix-as-12.txt, June 2007

[PSAMP-FMWK] D. Chiou, B. Claise, N. Duffield, A. Greenberg, M. Grossglauser, P. Marimuthu, J. Rexford, G. Sadasivan, "A Framework for Passive Packet Measurement" draft-ietf-psamp-framework-12.txt

[PSAMP-TECH] T. Zseby, M. Molina, N. Duffield, S. Niccolini, F. Raspall, "Sampling and Filtering Techniques for IP Packet Selection" draft-ietf-psamp-sample-tech-10.txt

[PSAMP-PROTO] B. Claise (Ed.), "Packet Sampling (PSAMP) Protocol Specifications", RFC XXXX. [Currently Internet Draft draft-ietf-psamp-protocol-09.txt, work in progress, December 2007].

[PSAMP-INFO] T. Dietz, F. Dressler, G. Carle, B. Claise, "Information Model for Packet Sampling Exports", draft-ietf-psamp-info-08.txt

[PSAMP-MIB] Dietz, T., Claise, B. "Definitions of Managed Objects for Packet Sampling", Internet-Draft work in progress, June 2006

10. Security Considerations

The IPFIX information model itself does not directly introduce security issues. Rather, it defines a set of attributes that may for privacy or business issues be considered sensitive information.

11. Contributors

Ganesh Murthy
Cisco Systems, Inc.
3850 Zanker Road
San Jose , CALIFORNIA 95134
United States

Phone: +1 408 853 7869
EMail: gmurthy@cisco.com

Marco Foschiano
Cisco Systems, Inc.
Torri Bianche-Faggio Bldg Lot H1
Via Torri Bianche 7
Vimercate 20059
Italy

Phone: +39 039 629 5244
EMail: foschia@cisco.com

12. Acknowledgements

The editors would like to thank the following persons for their reviews of the information elements specifications: Andrew Johnson, Gennady Dosovitsky, George Serpa, Mike Tracy, Nagaraj Varadharajan, Senthil Sivakumar, Stan Yates, Stewart Bryant and Roland Dobbins. The contributors wish to thank the following individuals for discussions and feedback: Bob Klessig, Neil McGill, Samer Salam, Yibin Yang, Ravi Samprathi and Prasanna Rajah.

13. Authors' Addresses

Paul Aitken
Cisco Systems, Inc.
96 Commercial Quay
Edinburgh EH6 6LX

Scotland

Phone: +44 131 561 3616
EMail: paitken@cisco.com

Benoit Claise
Cisco Systems, Inc.
De Kleetlaan 6a b1
Diegem 1831
Belgium

Phone: +32 2 704 5622
EMail: bclaise@cisco.com

14. Intellectual Property Statement

15. Copyright Statement

16. Disclaimer

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.