Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 30, 2014

P. Fan
China Mobile

July 29, 2013

# Requirements for Application Layer Information Export in IP Flow Information Export (IPFIX)
## draft-fan-ipfix-content-info-req-01

## Abstract

This document specifies requirements for exporting application layer information using IPFIX.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 30, 2014.

Table of Contents



## 1. Introduction

Our internet today carries a large variety of applications and services. Apart from layer 3 and layer 4 flow information, network administrators constantly rely on information in higher layers to monitor traffic flows. This kind of application related information is used in many aspects, e.g. network planning, operation, monitoring, analyzing, etc.

The IPFIX protocol provides us with ways to give network administrators flow information. A series of standards have been defined by IPFIX WG, including requirements [RFC3917], architecture [RFC5470], protocol specification [I-D.ietf-ipfix-protocol-rfc5101bis], and information model [I-D.ietf-ipfix-information-model-rfc5102bis]. IPFIX already provides Information Elements for every common Layer 4 and Layer 3 packet header field in the IETF protocol suite, basic Layer 2 information, basic counters, timestamps and time ranges, and so on, according to [I-D.draft-ietf-ipfix-ie-doctors]. However, application layer information export is not yet well standardized. Granular, well-defined information models that can be used in a universal, interoperable way to gather application layer information have not been specified.

This memo describes requirements for exporting application layer information of traffic flows, and intends to update [RFC3917].

## 2. Scope

The document describes requirements for exporting application layer information. By "application layer" we are actually referring to layers above the transport layer, and do not precisely classify a protocol into layer 5, 6 or 7.

The requirements and scenarios in this documents are based on practical needs. Flow monitoring and information export is done globally and statistically without specific targets, and must avoid violating RFC2804 regarding IETF policy on wiretapping.

## 3. Current Related Information Elements

There are a number of previously defined coarse-grained information elements that can be used or referred to when dealing with application layer information.

Application IEs: [RFC6759] defines a set of information elements used for export application information, including applicationDescription, applicationId, applicationName, classificationEngineId, applicationCategoryName, applicationSubCategoryName, applicationGroupName, etc. Applications in [RFC6759] are defined as networking protocols (can be layer 2 to layer 7) used by networking processes that exchange packets between them. These information elements give overall information of what applications are running on our network.

Packet Section IEs We have already several information elements that carry a series of octets in a packet/frame, e.g. ipHeaderPacketSection, ipPayloadPacketSection, mplsLabelStackSection, mplsPayloadPacketSection, etc. These information elements can even report octets from payload, subject to RFC2804. Note that the octets these information elements report start from the beginning of the measured packet/frame, but application layer information we talk about in this document is

likely to locate in any (even not fixed) place of a packet, and may not always locate in every packet.

# 4. Use cases

## 4.1. Internet Content Introducing in Data Centers

The Internet is operated by a number of ISPs (Internet Service Providers) and ICPs (Internet Content Providers). ISPs provide internet access service to subscribers and ICPs provide content. If internet content resources (web sites, service platforms, etc.) subscribers want to visit locate inside an ISP's network, then the





internet surfing traffic generated by subscribers will be restricted within the network; if resources are outside the network, then the traffic will be routed out of the network to the ICPs. For ISPs with little internet content resources, a large amount of internet traffic goes to other providers' networks, leading to

1. Pressure on the interconnecting links if bandwidth is limited;

2. User experience degradation when congestion occurs;

3. Interconnection fees if the ISP has to pay for the transit traffic.

The solution is to bring the content of ICPs into the ISP's own networks. Normally web sites are introduced and placed inside the data centers of an ISP, then the relevant internet traffic generated by subscribers will not go out of the network.

## 4.2. Web Site Performance Monitoring

Network administrators conduct the monitoring to evaluate the performance of web sites and user experience of internet access. A common way is to deploy probes at selected locations in the network and generate actively measurement traffic to visit web sites to be monitored. Some of the metrics and information needed include

For each web page element:

1. Durations, including DNS lookup, TCP connection, request

sending, waiting, response receiving, TTFB (Time To First Byte), etc.;

2. Success rate of downloading the elements;

3. Bytes sent and received by the browser in HTTP messages;

4. Specific information, e.g. method, content type, URL, referrer, etc.

For web page:

1. Web page loading duration;

2. Number of elements, DNS lookups, TCP connections;

3. Total bytes sent and received;





## 5. Problem Statement

### 5.1. Internet Content Introducing in Data Centers

The internet traffic is booming very fast these years, but usually the speed of building a new IDC is much slower. Thus for ISPs with limited IDC resources and urgent ICP introducing needs, it has to be considered carefully which web sites and which domain names (or hosts) of a web site should be introduced first. The basic principle is to give high priority to those "hot spots" which absorb more traffic, and the first thing to do is getting a list of hot spots.

With IPFIX today's routers on the interconnecting links can give network administrators a top-N list of outside IP addresses, indicating the destinations with the most traffic destined to them. But knowing the IP address is not enough, because:

1. The entity the IP address belongs to is not known;

2. Even if we can find out the owner of the IP address, the user of the IP address may be someone else, e.g. an ISP has an IP address of 1.2.3.4 and allocates it to a server of www.abc.com inside its

IDC;

3. IP address of a web site is subject to change; and

4. Most importantly, it is just not the routine to use IP addresses to go for negotiation. Marketing people negotiate with ICPs over the domain names (hosts) to be brought into the network, e.g. picture.abc.com & news.abc.com are of high priority while finance.abc.com & www.example.net are not so urgent.

## 5.2. Web Site Performance Monitoring

The current probe approach is an active way to do the monitoring, generating test traffic to the target web sites and measuring information. The performance monitoring procedure is done locally on probes, and a third-party platform that manages the probes is used to provide data integration and presentation. Export and storage of the results are done by vendors in proprietary ways, without standard definitions. Probes and platforms can not work in an interoperable way, and network administrators have to rely on third-party platforms to get test result data, with no means to achieve data records via the centralized NMS (Network Management System).

Another approach is to do passive monitoring on routers, though in this case some metrics will not be measured. This approach can be carried out at any or all locations of a network covering all





traffic, which is directly generated by users. Similar as the active approach, there is no standard way for IPFIX to export information needed for web site performance monitoring.

# 6. Requirements

This section describes requirements for exporting application information.

1. With IPFIX extended, information in protocols above transport layer is required to be exported based on needs.

2. The Metering Process should be able to parse certain fields in application protocols to get and export information needed.

3. The Metering Process should be able to do counting and timing for application protocols to be measured.

## 7. Security Considerations

TBD.

## 8. IANA Considerations

This memo includes no request to IANA.

## 9. Normative References


[I-D.draft-ietf-ipfix-ie-doctors]
Trammell, B. and B. Claise, "Guidelines for Authors and Reviewers of IPFIX Information Elements", draft-ietf-ipfix-ie-doctors-07 (Work in Progress), October 2012.

[I-D.ietf-ipfix-information-model-rfc5102bis]
Claise, B. and B. Trammell, "Information Model for IP Flow Information eXport (IPFIX)", draft-ietf-ipfix-information-model-rfc5102bis-10 (Work in Progress), February 2013.

[I-D.ietf-ipfix-protocol-rfc5101bis]
Claise, B., Trammell, B., Aitken, P., Bryant, S., Leinen, S., and T. Dietz, "Specification of the IP Flow Information eXport (IPFIX) Protocol for the Exchange of Flow Information", draft-ietf-ipfix-protocol-rfc5101bis-08 (Work in Progress), June 2013.

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







[RFC5470] Sadasivan, G., Brownlee, N., Claise, B., and J. Quittek, "Architecture for IP Flow Information Export", RFC 5470, March 2009.

[RFC6957] Claise, B., Aitken, P., and N. Ben-Dvora, "Cisco Systems Export of Application Information in IP Flow Information Export (IPFIX)", RFC 6957, November 2012.

Author's Address

Peng Fan
China Mobile
32 Xuanwumen West Street, Xicheng District
Beijing  100053
P.R. China

Email: fanpeng@chinamobile.com