opsawg
Internet-Draft
Intended status: Standards Track
Expires: 2 February 2026

X. Gao, Ed.
S. Zhang
China Unicom

1 August 2025

Export of terminal and application identification Information in IP Flow Information Export (IPFIX)

draft-gao-opsawg-ipfix-term-and-app-00

Abstract

This document specifies the extended information elements used in IPFIX (IP Flow Information Export) to export application layer information for identifying terminal and cloud application related information.

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 https://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 2 February 2026.

Copyright Notice

Table of Contents

1. Introduction

At present, the information related to terminal and cloud applications is crucial in the intelligent management of Internet traffic, especially in the end-to-end IPv6 network capability monitoring technology, [I-D.pang-v6ops-ipv6-monitoring-deployment-01] proposed that in order to accurately find the blocking points and sticking points of IPv6 traffic improvement, improve the end-to-end penetration level and service quality of IPv6 network, the network management system needs to master the end-to-end IPv6 capability support. In addition to the network forwarding equipment (such as routers) information, it also includes home terminals, and access applications. Currently, the information export of terminal and cloud applications has not been well standardized. This document specifies the information elements used for exporting terminal and cloud application information.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119][RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Problem Statement

In IPv6 end-to-end traffic monitoring, the identification of terminal types (including mobile phones, PADs, etc) can be analyzed from the User agent field of the HTTP packet, which describes the device used to access the internet; For the identification of cloud applications, it is also necessary to parse the seven layer information of the message, including the Host, URL and other fields in HTTP messages, SNI feature fields, session ID and other fields in HTTPS messages to identify the application. By exporting these fields and analyzing the data characteristics of network management, further evaluation of IPv6 capability support can be achieved.

4. New Information Elements

4.1. User-agent

Description：

The User-Agent request-header field contains information about the user agent originating the request. This is for statistical purposes, the tracing of protocol violations, and automated recognition of user agents for the sake of tailoring responses to avoid particular user agent limitations. Although it is not required, user agents should include this field with requests. The field can contain multiple product tokens and comments identifying the agent and any subproducts which form a significant part of the user agent. By convention, the product tokens are listed in order of their significance for identifying the application.

Reference：[RFC1945]

4.2. Host

Description：

The Host request-header field specifies the Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource (generally an HTTP URL). The Host field value must represent the naming authority of the origin server or gateway given by the original URL. This allows the origin server or gateway to differentiate between internally-ambiguous URLs, such as the root "/" URL of a server for multiple host names on a single IP address.

Reference：[RFC2616]

4.3. URL

Description：

A URL (Uniform Resource Locator) is a compact string representation used to identify and locate resources available via the Internet. It provides a standardized method for describing the location and access method of resources.

Reference：[RFC1738]

4.4. SNI

Description：

SNI is an extension to the TLS protocol that allows a client to indicate the hostname of the server it is contacting. This is particularly useful for servers hosting multiple virtual servers at a single underlying network address.

Reference：[RFC3546]

4.5. session ID

Description：

An arbitrary byte sequence chosen by the server to identify an active or resumable session state.

Reference：[RFC4346]

5. Security Considerations

TBD

6. IANA Considerations

The document makes a request to IANA to register the Information Elements defined in section 4.

7. Informative References

[I-D.pang-v6ops-ipv6-monitoring-deployment]
Pang, R., Zhao, J., Jin, M., and S. Zhang, "IPv6 Network Deployment Monitoring and Analysis", Work in Progress, Internet-Draft, draft-pang-v6ops-ipv6-monitoring-deployment-01, 4 July 2025, <https://datatracker.ietf.org/doc/html/draft-pang-v6ops-ipv6-monitoring-deployment-01>.

Authors' Addresses

Xing Gao (editor)
China Unicom
Beijing
China
Email: gaox60@chinaunicom.cn

Shuai Zhang
China Unicom
Beijing
China
Email: zhangs366@chinaunicom.cn