

**Requirements and Information Elements for Application Layer  
Information Export in IP Flow Information Export (IPFIX)  
draft-gao-opsawg-ipfix-term-and-app-01**

Xing Gao (China Unicom)

Shuai Zhang (China Unicom)

Changwang Lin (New H3C Technologies)

IETF-125

# Motivation and Objective

## Motivation

- **Problems:** In network operation management, relying solely on traffic information from the network layer (Layer 3) and transport layer (Layer 4) can no longer satisfy the requirements of refined operation and intelligent decision-making. Such basic information only reflects the routing, ports, and transmission status of data packets, **but fails to reveal the business attributes, user behaviors, and application intentions behind the traffic.**
- **Solutions:** Application layer information enables accurate identification of traffic business types and user behavior preferences, providing a critical foundation for network planning, resource scheduling, and user experience optimization.

## Objective

This draft solves the limitation of traditional IPFIX in only collecting network/transport layer data by **defining the export of IPFIX application layer information. Through standardized collection of core application-layer characteristics such as HTTP/HTTPS, in-depth mining of user behavior can be achieved, while satisfying the demands for refined network resource scheduling and intelligent traffic monitoring and management.**

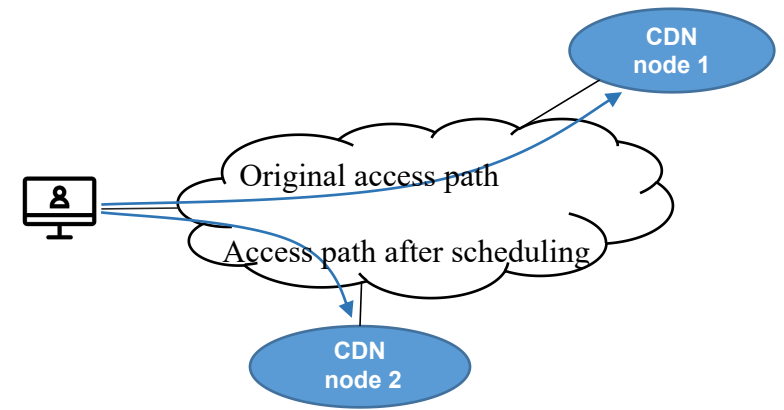
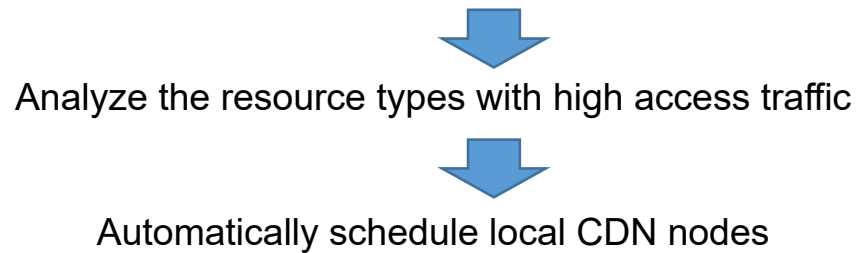
*Note: The information elements specified in this draft include HTTP and HTTPS, and other application layer information is not within the scope of this draft.*

# Sample Use Cases

## Case1:CDN content introduction and traffic scheduling optimization

There is a large amount of HTTP/HTTPS traffic in the backbone network or metropolitan area network of the operator. Traditional IPFIX can only see the IP, port, and traffic size, and cannot identify the business type and content, making it difficult to accurately introduce content and schedule traffic. **By exporting application layer information elements, it is possible to identify and analyze the types and frequencies of resources accessed by users.** The network management platform automatically schedules high traffic and high access proportion businesses to local CDN nodes, reducing cross provincial/cross network traffic, reducing cross network bandwidth costs, improving user experience, and achieving precise content introduction and traffic scheduling.

Export application layer information (including domain names, etc.) based on IPFIX



# Sample Use Cases

## Case2: IPv6 Network Deployment Monitoring and Analysis

[I-D.pang-v6ops-ipv6-menitoring deployment-05] suggests that in order to improve the end-to-end connectivity and service quality of IPv6 networks, it is necessary to identify where the bottleneck of IPv6 networks lies, and there may be blocking points in user terminals, network nodes, and accessed applications. By exporting application layer information (including terminal and application information) based on IPFIX, end-to-end IPv6 support in the entire network can be identified and analyzed.

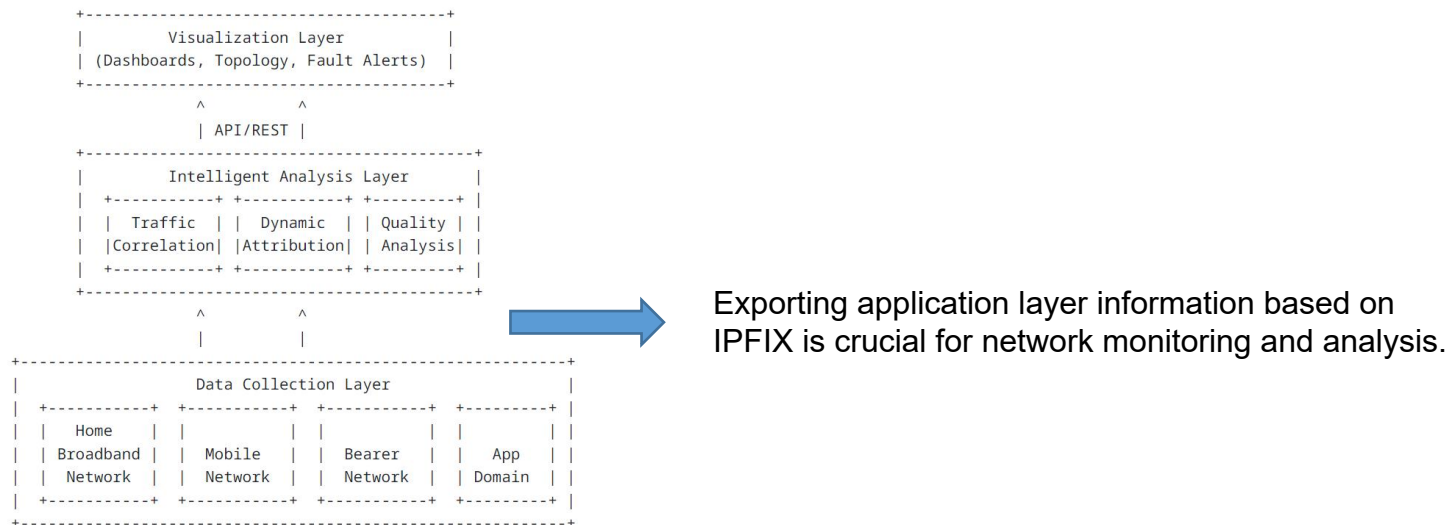


Figure 1: IPv6 Network End-to-End Monitoring and Analysis Architecture

# New Information Elements

4.	New Information Elements	
4.1.	httpUserAgent	
4.2.	httpRequestHost	
4.3.	httpRequestReferer	
4.4.	httpRequestAccept	
4.5.	httpStatusCode	
4.6.	httpRequestMethod	
4.7.	httpRequestTarget	
4.8.	httpMessageVersion	
4.9.	httpContentType	
4.10.	httpReasonPhrase	
4.11.	httpResponseCacheControl	
4.12.	httpResponseETag	
4.13.	httpResponseServer	
4.14.	tlsSNI	
4.15.	tlsVersion	
4.16.	tlsClientHelloCipherSuite	
4.17.	tlsClientHelloSSLExtension	
4.18.	tlsClientHelloEllipticCurve	
4.19.	tlsClientHelloEllipticCurvePointFormat	

- 4.1-4.8 fields are related to HTTP/HTTPS request packets and can be used for business identification and access behavior analysis;
- 4.9-4.13 are related to HTTP/HTTPS response packets and can be used for service quality analysis and optimization;
- 4.14-4.19 are HTTPS handshake-related fields, enabling client feature identification and detection of abnormal network behavior without decrypting traffic.

## Note:

- HTTP adopts a plaintext transmission mechanism, and relevant fields can be directly extracted and exported;
- HTTPS first completes encryption negotiation through TLS handshake, and then transmits HTTP messages. The encrypted content of HTTP messages may not have access to their related fields.

- Any comments or any suggestions?

Thank you