HTTPBIS Working Group
INTERNET-DRAFT
Intended Status: Informational
Expires: May 3, 2016

L. Deng
China Mobile
Y. Xia
China SARFT
S. Duan
CATR

November 2, 2015

Use-cases for Traffic Tagging
draft-deng-httpbis-urlid-01

Abstract

This document discusses the motivation and use-cases for coding third-party aware tags for content/source related information into resource retrieval process.

Table of Contents

1 Introduction

The document discusses the motivation and use-cases for coding third-party aware tags for content/source related information into resource retrieval process.

2 Motivating Senarios

2.1 Content Caching

As stated earlier, cache systems are considered to be an effective way to reduce the prohibitive expense for cross-boundary traffic from large ISP with most ICPs to small ISPs providing local services to a specific group of subscribers. The cache system automatically buffers the hotspot resources locally and reduces the traffic from the large operators by feeding the requested content locally.

However, observed from the reality of operating, the local cache system can't fully implement traffic localization, as there are vast user requests redirected to other operators by DNS, even when the requested content is actually cached locally.

The main reason is that the work pattern of cache system is fully passive and the cache system uses the DPI technology to acquire the URL to identify for buffered content and match them with subsequent content requests, which causes undesirable cache misses in the following two cases:

On the one hand, for video websites using the anti-stealing-link mechanism, which updates the URL for the same content periodically with new ones, subsequent requests are therefore subject to change even from the same website.

On the other hand, for the requests from the local subscribers to different websites, the cache system cannot recognize a content hit even if the content they are requesting are identical, as their URLs are likely to be different.

2.2 Reverse Charging

The dominating billing method is subscriber-oriented model, which is used by the operator to charge the subscriber for the volume of or expected bandwidth for the Internet traffic he consumes for a given period of time (e.g. on a monthly basis). In practice, such model is implemented by the network devices monitoring the flows targeted to or originated from a given subscriber (e.g. local IP address).

However, reverse charging is becoming a desirable new billing method,

which is motivated from ICPs, who want to cooperative with the ISPs to enable free-access to its content/service from the subscribers to attract users, especially the mobile subscribers. The key to enable such billing model is how to effectively distinguish the traffic flows belonging to the same content/application which might be comprised of complex groups of IP flows from others. The current subscriber-based billing model is not very helpful in such scenario.

3 Requirements

3.1 Identifying the content

In order to improve the hit ratio and actively push the hot resources to the local subscribers, the cache system need a succinct way to learn the buffered contents and can judge the hot content according to the actual content information.

3.2 Identifying the source

To enable flexible reverse charging, we need a third party recognizable tag of the traffic for the charging GW located between the client and server, which helps in recognition of its source and billing model, and other features to enable other cultivated transport services, e.g. QoS for selected content types for a given ICP.

4 Challenges

4.1 Identifiers of the content

Current identifiers for web content (e.g. URL) is based on its location, rather than the real content. Content tagging is expected to be helpful to address these requirements. E.g. to mark the content information and encode this flag/tag into the content's URL, which identifies its binary content and other application metadata. The cache system can know the exact content by analyze the content flag in the URL link and need no changes to any protocol.

4.2 On identifying the source

It is expected that tag for the source in the reverse charging case is independent of IP address and above of IP layer, since source IP is not working for CDN cases.

The tag is expected to also provide information about content type for finer-grained charging policies, as the diversity of network applications has high demand for the charging policy flexibility,

e.g. a single application may produce both video traffic and audio traffic, which decides to complain its upgraded video service for free while keeping its commercial voice service intact.

4.3 On tagging the encrypted traffic

Another big challenge for third-party resource tagging is encryption. If the tag is added at the application layer and encrypted end-to-end, that would block a cache or charging GW to retrieval the embedded information.

4 Discussion

5 Security Considerations

TBA.

6 IANA Considerations

There is no IANA action in this document.

7 Acknowledgements

TBA.

8 References

8.1 Normative References

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

Authors' Addresses

Lingli Deng
China Mobile

Email: denglingli@chinamobile.com

Yong Xia
China SARFT

Email: xiayong@abs.ac.cn

Shihui Duan
China Academy of Telecommunication Research of MIIT

Email: duanshihui@catr.cn