

Network Working Group
Internet Draft
Intended status: Standard Track
Expires: January 21, 2015

A. Wang
China Telecom
S. Jiang
Huawei Technologies Co., Ltd
July 20, 2014

IPv6 Flow Label Reflection
draft-wang-v6ops-flow-label-refelction-01.txt

Abstract

IPv6 Flow Label field in IPv6 packet header is designed to differentiate the various traffic flow session within network. The current definition of IPv6 Flow Label focuses mainly on how the packet source forms the value of this field and how the forwarder in-path treats it. There is no analysis on the relation between the flow label from source nodes and its corresponding value in return packet. This draft analyzes the requirements for flow label reflection between the upstream session and the corresponding downstream session. Based on the analysis, the flow label reflection mechanism is proposed in this document.

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 21, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Conventions used in this document	3
3.	Flow Label Reflection Requirements	3
3.1.	Summary of the current usage for IPv6 Flow Label	3
3.2.	Requirements of Flow Label Reflection	4
3.2.1.	DS-Lite deployment Scenario	4
3.2.2.	Deep Packet Inspection Scenario	6
3.2.3.	End to End QoS Deployment Scenario within Mobile Network	6
4.	Recommendation and Benefit of Flow Label Reflection Mechanism	7
5.	Detail Process for Flow Label Reflection	8
5.1.1.	DS-Lite environment	8
5.1.2.	NAT64 environment	8
5.1.3.	End to End IPv6 communication environment.....	9
5.2.	Influence to the current usage of IPv6 Flow Label	9
6.	Conclusions	9
7.	Security Considerations	9
8.	IANA Considerations	10
9.	Acknowledgments	10
10.	References	10
10.1.	Normative References	10
10.2.	Informative References	10

Internet-Draft

Flow Label Reflection

July 2014

1. Introduction

IPv6 flow label [[RFC6437](#)] is designed to differentiate the flow session of IPv6 traffic; it can accelerate the clarification and treatment of IPv6 traffic by the network devices in its forwarding path. Currently, the usage of this field mainly focus on the traffic load-balance in ECMP (Equal Cost Multi-Path) environment [[RFC6438](#)] or the server load balance [[RFC7098](#)], these usages only exploit the characteristic of IPv6 flow label field in one direction, and do not consider the requirement to correlate the upstream and downstream traffic of one session together to create new service model, to simply the traffic policy deployment and to increase the accuracy of network traffic recognition.

In this draft, we analyze the requirements of the flow label reflection mechanism in several scenarios. There is administration benefit for keeping flow label unchanged in the downstream and upstream of one IPv6 traffic session. The details IPv6 flow label reflect process in DS-Lite, NAT64 [[RFC6146](#)] and IPv6 end-to-end communication environment are also given.

Further deployment requirements and solutions are welcomed and will be studied later.

2. 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 [[RFC2119](#)].

3. Flow Label Reflection Requirements

3.1. Summary of the current usage for IPv6 Flow Label

[[RFC6438](#)] describe the usage of IPv6 Flow Label for ECMP and link aggregation in Tunnels, it mainly utilize the random distribution characteristic of IPv6 flow label. [[RFC7098](#)] also describe similar

usage case in server farm. All these usage scenarios consider only the usage of IPv6 flow label in one direction, and do not utilize fully the core definition and role of IPv6 flow label for one session. From the point view of service provider, the upstream and downstream of one session should be handled together, then give them the same label value will be more beneficial.

Following paragraph analyzes several scenarios that require IPv6 flow label reflection mechanism. Other use case needs to further study.

[3.2.](#) Requirements of Flow Label Reflection

This section describes some scenarios that require the IPv6 flow label reflection in IPv6 source and destination nodes. Other similar situations may be required further study.

[3.2.1.](#) DS-Lite deployment Scenario

During IPv6 transition stage, some Internet Service Providers the DS-Lite [[RFC6333](#)] technology to accelerate the deployment of IPv6 within their network. DS-Lite has the beneficial to eliminate the needs to assign the IPv4 address to the subscribers and simplify the administration of network, but it has one disadvantage that encapsulates all IPv4 traffic from one customer into IPv6 packet and the router in-path, such as BRAS, CR etc. cannot see the inner IPv4 destination information.

On the other hand, the Internet Service Providers want to differentiate the traffic within their transport pipe, which is based on the requirement from upper CP/SP (Content provider). The general architecture to achieve this goal is illustrated in Figure-1:

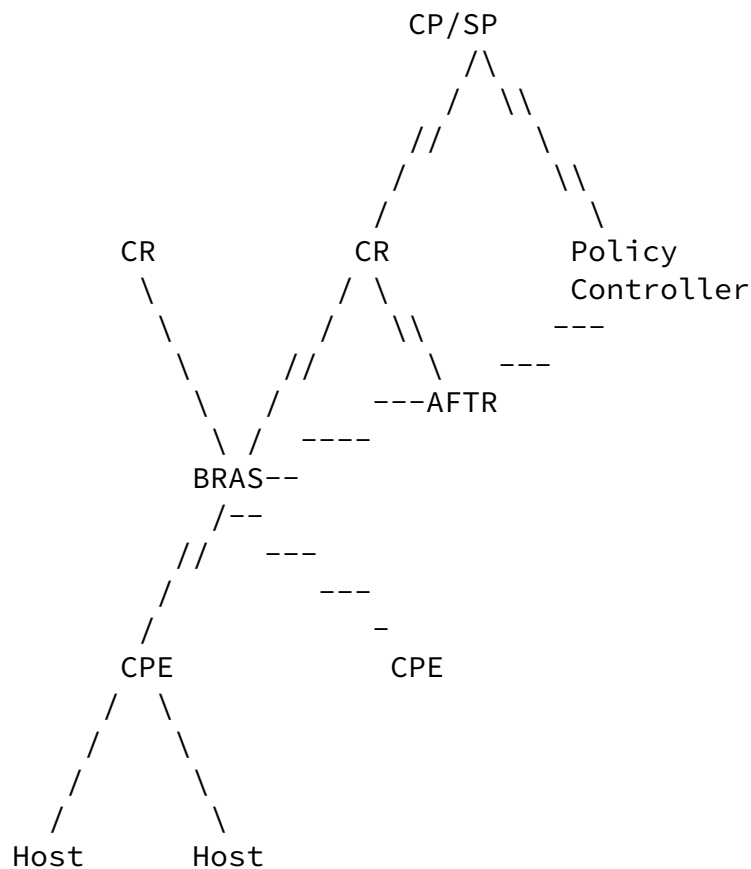


Figure-1: DS-Lite Deployment Scenarios

Within Figure-1, CPE acts as B4 [[RFC6333](#)] to encapsulate the IPv4 traffic from host under it into IPv6 packet. According to the current IPv6 node requirement, CPE is responsible to allocate one random/well distribution value to the flow label, to indicate the

different IPv4 flow from host is belong to different flow session.

The encapsulate IPv6 traffic pass through BRAS and CR, ends in AFTR [[RFC6333](#)] which will decapsulate IPv6 traffic into IPv4 packet and return it to CR, the CR will pass the decapsulated IPv4 packet to CP/SP. If the CP/SP wants more bandwidth or quick process, they will deliver the destination IP and port information to the "Policy Controller", which will control the AFTR and then to lift the bandwidth limit on BRAS.

For BRAS to act correctly to the appointed IPv4 traffic, it should know the corresponding IPv6 flow label. If the upstream IPv6 flow label is different from the downstream IPv6 label, the ACL lists in BRAS will be quite complex, the upstream and downstream of one session must be processed separately. This will increase the burden of service provider to deploy intelligent network policy.

<Wang>

Expires January 15, 2015

[Page 5]

Internet-Draft

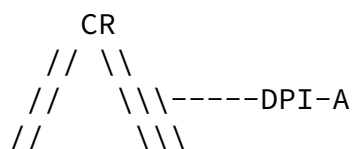
Flow Label Reflection

July 2014

[3.2.2.](#) Deep Packet Inspection Scenario

Internet service providers are now deploying more DPI (Deep packet inspection) devices within their network to accomplish the visualization of traffic type in their communication pipe and wish to optimize their network structure based on these information. The accuracy of the DPI devices' traffic recognition will influence the effect of network optimization and controlling policy.

To increase the traffic recognition rate, the DPI device should track the upstream and downstream of one session simultaneously, in order to find the symptoms of various traffic, especially for P2P traffic. If the IPv6 flow label of upstream and downstream is different, and the three tuple <IPv6 source address, IPv6 destination address, flow label> is used to load balance among different links between BRAS and CR, as illustrated in Figure-2, the upstream and downstream of one session will be distributed into different links and then to different DPI devices(DPI-A or DPI-B), thus increases the difficult of traffic recognition that is based on the correlation of downstream and upstream of one session.



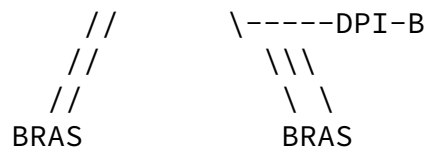


Figure-2 Deep Packet Inspection Deployment Scenarios in IPv6-Only Environment

3.2.3. End to End QoS Deployment Scenario within Mobile Network

Under the mobile network environment, the service provider can control the traffic parameter from UE directly. Based on the common architecture as illustrated in Figure-3 below for end to end QoS deployment within mobile networks, UE will get the QCI parameter from PCRF, and the traffic from this UE will be treated differently according to its service subscription. If the UE and PCRF have the same mapping algorithm, the QCI parameters can be mapped to the IPv6 flow label in underlying transport layer. By keeping the value of IPv6 flow label in upstream and downstream same, and based on the mapping information and policy from PCRF, the transport devices can treat the required flow different very easily.

<Wang>

Expires January 15, 2015

[Page 6]

Internet-Draft

Flow Label Reflection

July 2014

Specially, under the situation of UE to UE communicate directly, the traffic initiated by the privilege user will be processed in high priority, even it communicate with one low precedence user; and the traffic initiated by the normal user will be processed in default queue, even it communicate with one privilege user. This traffic model matches with the service provider's business model and can be easily accomplished.

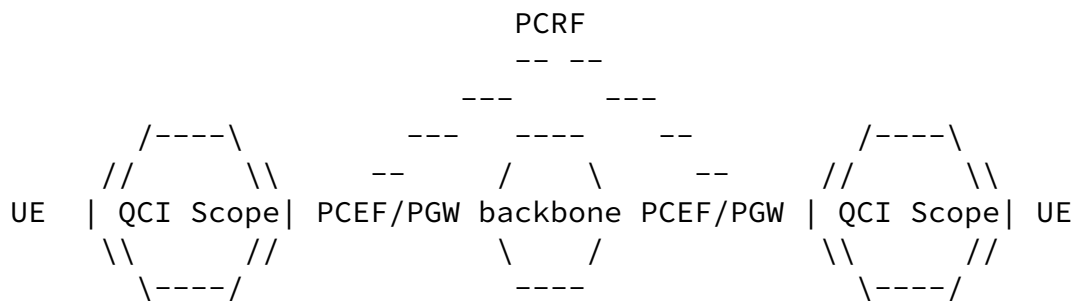


Figure-3 End to End QoS deployment within Mobile Network

[4.](#) Recommendation and Benefit of Flow Label Reflection Mechanism

Based on the scenarios described above, we propose the following solution:

1. The value of IPv6 Flow Label SHOULD be reflected and kept unchanged by the receiving IPv6 node.
2. Under such reflection mechanism, the IPv6 Flow Label will be used unambiguously to indicate one session's upstream and downstream traffic:
 - a) The service provider can easily apply the same policy to the bi-direction traffic of one interested session;
 - b) The traffic analyzer can also easily correlate the upstream and downstream of one session to find the symptoms of various internet protocol.
 - c) The service provider can offer differentiated service based on the user's privilege condition and their service in use, make the Non-equivalent service possible under the end-to-end communication model in mobile network environment.
3. The generation method of IPv6 flow label in source IPv6 node and the forward behavior are still recommended to follow the

<Wang>

Expires January 15, 2015

[Page 7]

Internet-Draft

Flow Label Reflection

July 2014

guidelines in [RFC 6437](#), that is the IPv6 flow label should be generated randomly and distributed enough, the devices in the traffic forwarding path should not change it.

[5.](#) Detail Process for Flow Label Reflection

[5.1.1.](#) DS-Lite environment

Under DS-Lite environment, the B4/CPE and AFTR are the two ends of IPv6 communication:

- a) B4/CPE is responsible for the generation of IPv6 packet, and is responsible for the initial value of IPv6 flow label. Because all IPv4 traffic from it is encapsulated into one IPv6 tunnel packet, the value of IPv6 flow label should distinguish the

inner different IPv4 flow. Recommending algorithm is to use the 5-tuple of IPv4 traffic as the input of hash function.

- b) AFTR is responsible for the decapsulation of IPv6 traffic. The original IPv6 flow label should be kept in the stateful table in AFTR, along with the mapping entry of "private IPv4 source/port, IPv6 source address, public IPv4 source/port, protocol".
- c) Once the responsible IPv4 traffic back to AFTR, it should check the above mapping table, NAT and encapsulate the IPv4 traffic, set the IPv6 flow label of returned encapsulated IPv6 packet to the previous stored value.

[5.1.2.](#) NAT64 environment

Under NAT64 environment, the IPv6 host and the NAT64 device is the two IPv6 communication ends:

- a) IPv6 host is responsible for the generation of IPv6 packet, and is responsible for the initial value of IPv6 flow label. Recommending algorithm is to use the 5-tuple of IPv6 traffic as the input of hash function.
- b) NAT64 is the other end of IPv6 communication session. It should record the original value of IPv6 flow label in upstream in its NAT table, along with the mapping entry of "IPv6 source address/port, public IPv4 source address/port, protocol"
- c) Once the responsible IPv4 traffic back to NAT64 device, it should retrieve the corresponding original value of IPv6 flow

label in the above mentioned mapping table, put it in the header of downstream converted IPv6 traffic.

[5.1.3.](#) End to End IPv6 communication environment

It is simpler to do IPv6 flow label reflection under the end to end Ipv6 communication environment:

- a) IPv6 source host is responsible for the generation of IPv6 packet, and is responsible for the initial value of IPv6 flow

label. Recommending algorithm is to use the 5-tuple of IPv6 traffic as the input of hash function.

- b) IPv6 destination host just copy the original IPv6 flow label to its corresponding field in reply packet.
- c) There is no need to keep the value of IPv6 flow label in forwarding path.

[5.2.](#) Influence to the current usage of IPv6 Flow Label

There is no any influence to the current proposed usages of IPv6 flow label.

[6.](#) Conclusions

IPv6 flow label reflection mechanism makes the downstream and upstream of one session be easily recognized, let the service provider take the full control of one session's bi-direction traffic and apply the same traffic policy to them. It also let the correlation of traffic and then the recognition of various traffics easier. Based on such mechanism, the service provider can also offer Non-equivalent service in IPv6 end-to-end communication environment, especially in the IPv6-based mobile network environment.

[7.](#) Security Considerations

In order to keep the IPv6 flow label unchanged and same in the upstream and downstream of one session, the in-path devices, which is required in the IPv6 transition period, such as AFTR/NAT64 etc. should be required to store the IPv6 flow label value, retrieve and restore it in the downstream traffic. This may increase the burden of such stateful devices within service provider's network and lower the anti-attack capabilities of these devices. This threat exists only in the transition period and will disappear in the IPv6 end-to-end communication period.

[8.](#) IANA Considerations

There is no additional IANA requirement for this requirement.

[9.](#) Acknowledgments

Valuable comments were received from Brian Carpenter.

This document was prepared using 2-Word-v2.0.template.dot.

10. References

10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC6146] M. Bagnulo, P. Matthews, I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers" [RFC 6146](#), April 2011
- [RFC6333] A. Durand, R. Droms, J. Woodyatt, Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", [RFC6333](#), August 2011
- [RFC6437] S. Amante, B. Carpenter, S. Jiang, J. Rajahalme, "IPv6 Flow Label Specification", [RFC 6437](#), November 2011.
- [RFC6438] B. Carpenter, S. Amante, "Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels", [RFC 6438](#), November 2011.

10.2. Informative References

- [RFC7098] B. Carpenter, S. Jiang, W. Tarreau, "Using the IPv6 Flow Label for Load Balancing in Server Farms", [RFC 7098](#), January 2014.

Authors' Addresses

Aijun Wang
China Telecom Cooperation Limited Beijing Research Institute
No.118, Xizhimenneidajie, Xicheng District, Beijing, 100035, China

Phone: 86-10-58552347
Email: wangaj@ctbri.com.cn

Jiang Sheng
Huawei Technologies Co., Ltd
Q14, Huawei Campus, No.156 Beiqing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: jiangsheng@huawei.com