IPv6 Flow Label Reflection

draft-wang-6man-flow-label-reflection

IETF 91 6man WG

November, 2014

Sheng JIANG (Speaker, co-author)
Aijun Wang(author)

IPv6 Flow Label Reflection Behavior

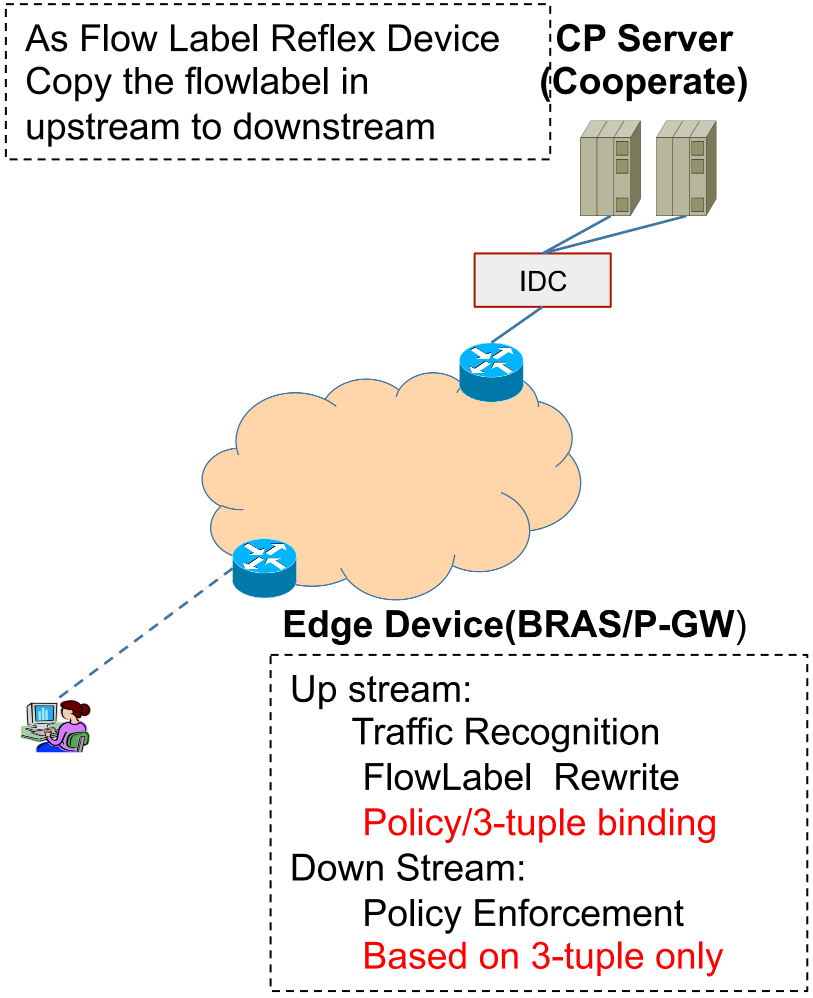
- The idea is straightforward:
  - A network device copies the value of flow label from a IPv6 flow into a corresponding return IPv6 flow.
  - On the Flow Label Reflection Device, the value of IPv6 Flow Label from received packets SHOULD be copied into the corresponding flow label field in return packets.
  - The network traffic recognition devices, or devices that may have differentiated operations per flow, SHOULD recognize and analyze network traffics based on 3-tuple of {dest addr, source addr, flowlabel}. It SHOULD consider the traffics that have same flow label value and reversed source/dest addr as upstream and downstream of the same flow, match them together to accomplish the traffic recognition process.

Potential Benefit of Flow Label Reflection

- **With flow label reflection mechanism, the IPv6 Flow Label could be used to correlate the upstream and downstream packets of bi-directional traffics:**
  - It makes the downstream and upstream of one session be easily recognized. It makes the correlation of traffic and then the recognition of various traffics easier.
  - The network operator can easily apply the same policy to the bi- directional traffic of one interested session.
  - The traffic analyzer can also easily correlate the upstream and downstream of one session to find the symptoms of various internet protocols.

Flow Label Reflection on CP servers (Applicable Scenarios 1)

- **The access edge devices of service provider scrutinize the subscriber's upstream IPv6 traffic and record the binding of 3-tuple and traffic-specific policy. If the flow label is zero, the access edge devices must rewrite the flow label value according to local policy.**
- **Flow label reflection on CP servers**
- **Recognition based on the 3-tuple of {dest addr, source addr, flowlabel} would reduce the consumption of recognition and make the correlation process much easier.**
- **Note: this mechanism may not reliable when the CP servers are not directly connected to the service provider**



As Flow Label Reflex Device
Copy the flowlabel in
upstream to downstream

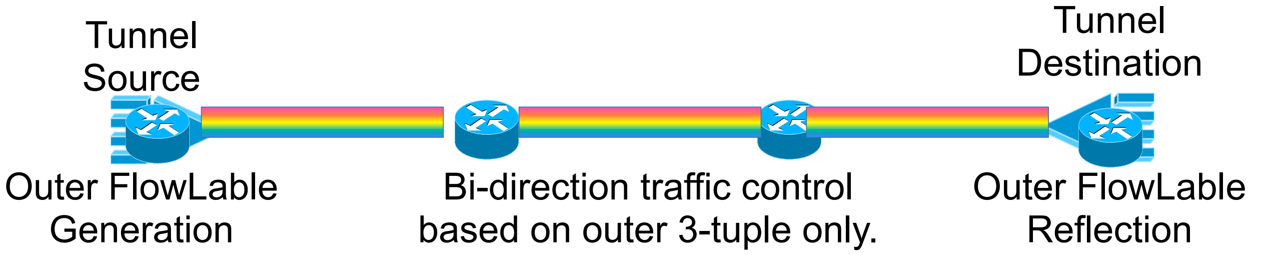
CP Server
(Cooperate)

Edge Device(BRAS/P-GW)

Up stream:
Traffic Recognition
FlowLabel Rewrite
Policy/3-tuple binding
Down Stream:
Policy Enforcement
Based on 3-tuple only

Flow Label Reflection for Bi-direction Tunnels (Applicable Scenarios 2)

- **The tunnel initiating devices should generate different flow label values for different inner flow traffics**
- **The tunnel end devices would be the Flow Label Reflection Devices. They record the flow label value from received tunnel packets, and copy it to the corresponding flow label field in return packets, which can be recognized by 5-tuple or 3-tuple of the inner packet**
- **the intermediate network device can easily distinguish the different flow within the same tunnel transport link and correlate bi-direction traffics of same flow together**



Flow Label Reflection on Edge Device (Applicable Scenarios 3)

- **Assuming the flow label reflection mechanisms have been applied on peer host, the service provider could always use it for bi-directional traffic recognition.**
- **However, there is no guarantee the flow label would not be changed by intermediate devices in other domains.**
- **The edge devices play as the (backup) Flow Label Reflection Devices.**
- **They record the flow label value from the packets that leave the domain. When the corresponding flow label field in return packets are recognized by 5-tuple or 3-tuple at the edge devices, the edge devices should check the flow label as below:**
  - if the flow label matches the record value, it remains;
  - if the flow label is zero, the edge devices copy the record value into it;
  - if the flow label is non-zero, but does not matches the record value, the edge devices can decide the flow label are modified by other intermediate devices (with the assumption the peer host has reflect the original flow label), then restore the flow label using the record value.

Supporting in Linux

Linux netdev, ipv6 model has been added an IPV6_FL_F_REFLECT_flag to IPV6_FL_A_GET, 2014 January.

by Florent Fourcot

Modified include/linux/ipv6.h

include/uapi/linux/in6.h

net/ipv6/ip6_flowlabel.c

net/ipv6/tcp_ipv6.c

Linux-based end hosts or network devices can easily use such flag to accomplish the Flow Label Reflection mechanism.

Security Consideration and Possible Attack

- The IPv6 Flow label is untrusted:
  - ✓ The policy controller should interact with the IPv6 host, to ensure this randomly generated value will be trusted. And it may be rechecked by the ingress nodes.
- The IPv6 Flow label is forged:
  - ✓ We only exploit the random characteristic of this value. The value would not be meaningful after the associated flow ends.
- Man-in-Middle attack:
  - ✓ Flow label reflection mechanism is more useful in a provider network, which can be considered as a closed network and a lower-threat environment.
- This document has mainly considered single administrative domain scenarios only

WG adoption?

Comments, Reviews & Contribution are appreciated!

Thanks！