IPv6 Flow Label Reflection

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

IETF 92 6man WG

March, 2015

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

IPv6 Flow Label Reflection Mechanism

- Copy the value of flow label from a IPv6 **upstream flow** into a corresponding **downstream** flow.
- Correlate the upstream/downstream packets via **3-tuple of {dest addr, source addr, flowlabel}.**
- Simplify the process on the network traffic recognition devices, or devices that needs to apply the same policy to the bi- directional traffic of one flow.
  - Otherwise, such actions must rely on the 5-tuple of one packet, which requires the device to parse into the IPv6 extend headers.

- Already supported in Linux (IPV6_FL_F_REFLECT_flag ,January 2014), so Linux-based end hosts or network devices can easily use such flag to accomplish the Flow Label Reflection mechanism

Applicable Scenarios

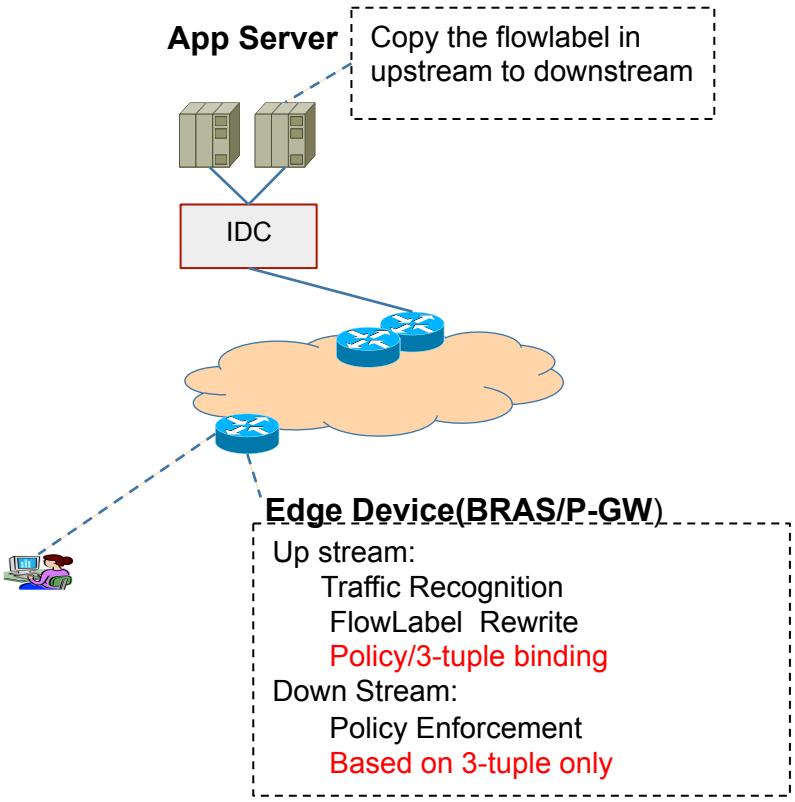

Fig.1 Flow Label Reflection on the Application/Content Provider Server

Fig.2 Flow Label Reflection on Tunnel Ends

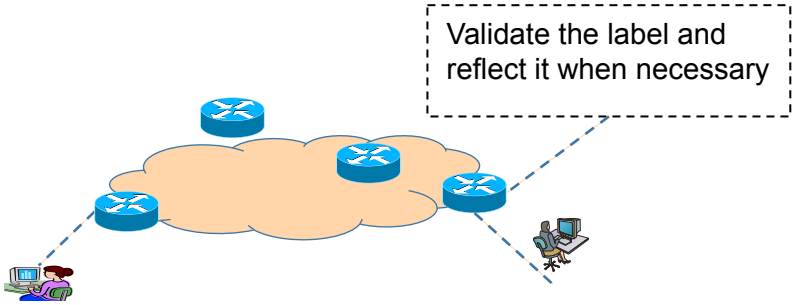

Fig.3 Flow Label Reflection on network edge device

More detail information in http://tools.ietf.org/html/draft-wang-6man-flow-label-reflection-01

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, in which the above security issues are minimum.**

Is this useful work? Interests from WG?

Comments, reviews & contributions are appreciated!