IPv6 Flow Label Reflection

draft-wang-v6ops-flow-label-reflection

IETF 90 V6OPS WG

July, 2014

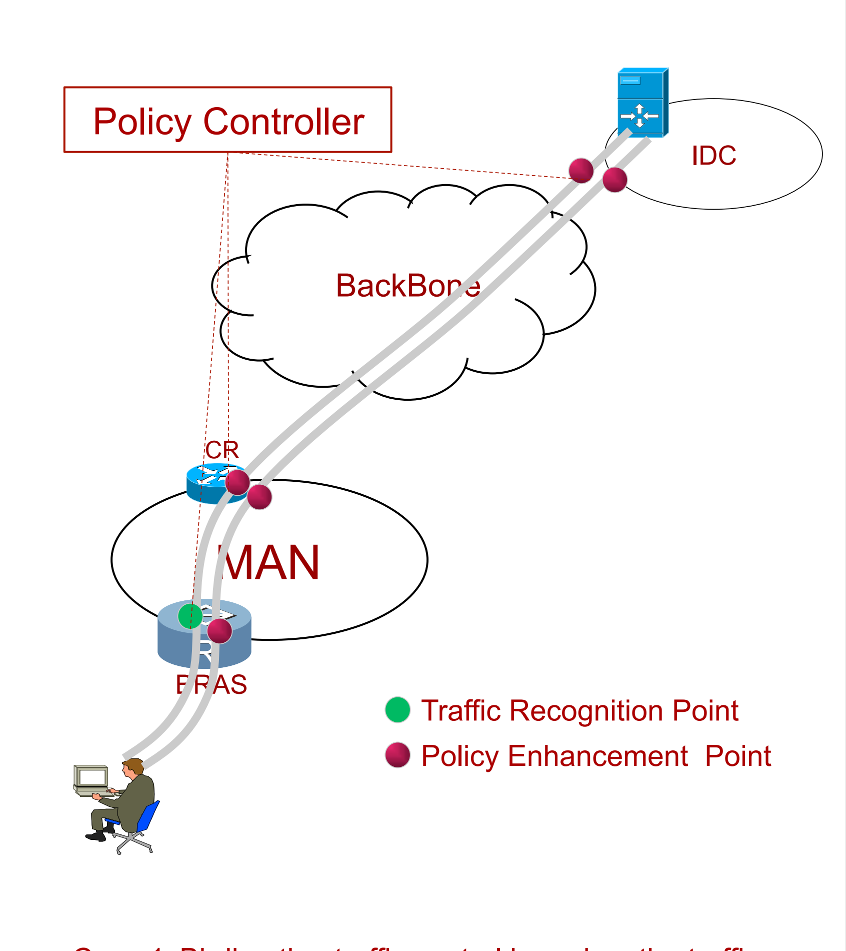
Sheng JIANG (Speaker, co-author)
Aijun Wang(author)

What is IPv6 Flow Label Reflection?

- The idea is straightforward:
  - Let the value of IPv6 flow label be same in upstream/downstream packet of one session.
  - Only the sender of the IPv6 packet will generate this value in random, the receiver of IPv6 packet will keep it unchanged and reflect it in the reply packet.
  - It should be supported by the host operation system, carrier middle devices (such as CGN/AFTR etc.)

The benefits of IPv6 Flow Label Reflection-1

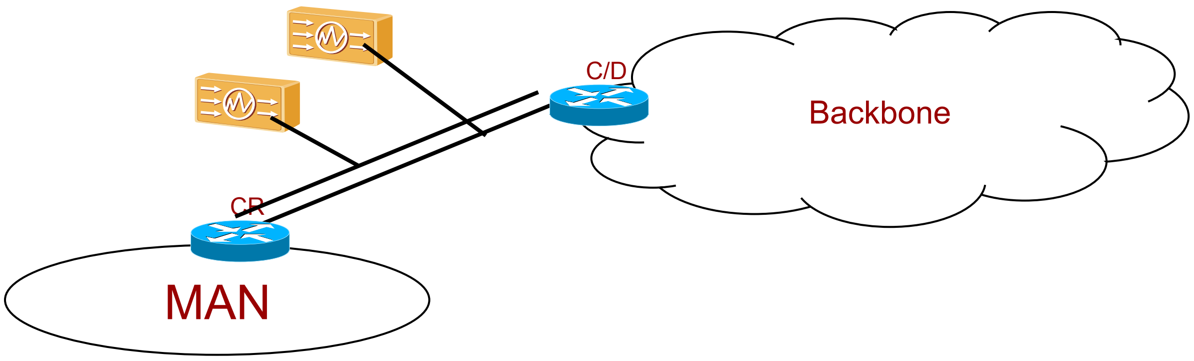
- With the characteristic of IPv6 Flow Label Reflection, the service provider can easily control the bi-direction traffic, based only on the traffic recognition result in one direction.
- Recognition in one direction, control and the same traffic handling policy for both directions.



Case 1：Bi-direction traffic control based on the traffic recognition result in one direction

The benefits of IPv6 Flow Label Reflection-2

- With the characteristic of IPv6 Flow Label Reflection, the recognition rate of IPv6 packet for DPI devices will be improved.
- The upstream and downstream packet of one session will all go through the same link, to the same DPI device.
- The correlation of up/down stream packet in one session will be more easily.



Case 2：The traffic recognition accuracy will be raised if up/down stream pass the same link and same DPI device.

The benefits of IPv6 Flow Label Reflection-3

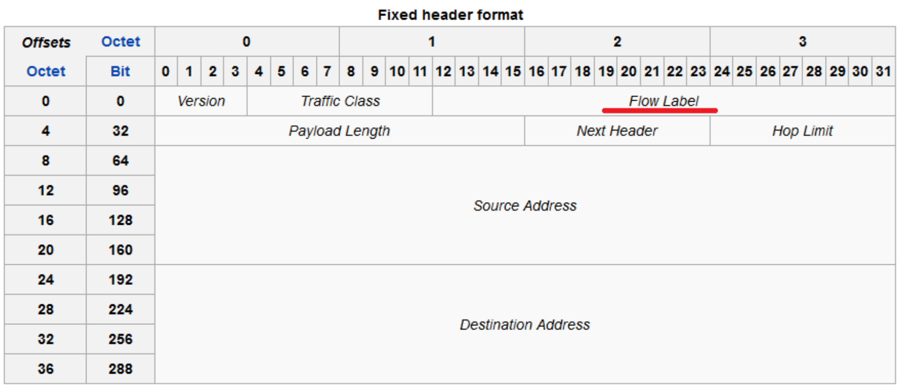
- With the characteristic of IPv6 Flow Label Reflection, the service provider can even deploy some interesting differential service:
  - Only the bi-direction traffic initiated by high priority user will be guaranteed, the low priority user can’t get this service, even it is talked to the high end user.
  - This can drive the differential service be widely accepted
  - The detail of such signaling process is another topic.

Case 3：In C2C communication scenario, the service traffic initiated by the high-priority user will be guaranteed in two directions.

Why use IPv6 Flow Label Reflection?

- If the IPv6 Flow Label in bi-direction traffic is different, previously mentioned requirements can only be met via the traditional 5-tuple information. But for IPv6 packet, these information is located at extension header, not in the IPv6 fix header.

- IPv6 Flow label could be used to assist the bi-direction traffic correlation. It is unique in IPv6



Fixed header format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				Traffic Class								Flow Label																			
4	32	Payload Length																Next Header								Hop Limit							
8	64	Source Address																															
12	96																																
16	128																																
20	160																																
24	192	Destination Address																															
28	224																																
32	256																																
36	288																																

Flow Label (20 bits) Originally created for giving real-time applications special service. The flow label when set to a non-zero value now serves as a hint to routers and switches with multiple outbound paths that these packets should stay on the same path so that they will not be reordered.

Currently, the flow label is used only to label the traffic in one direction, to let the IPv6 traffic be equally distributed within ECMP links.

Considered Situations

IPv6 Flow Label Reflection Process in different scenarios:

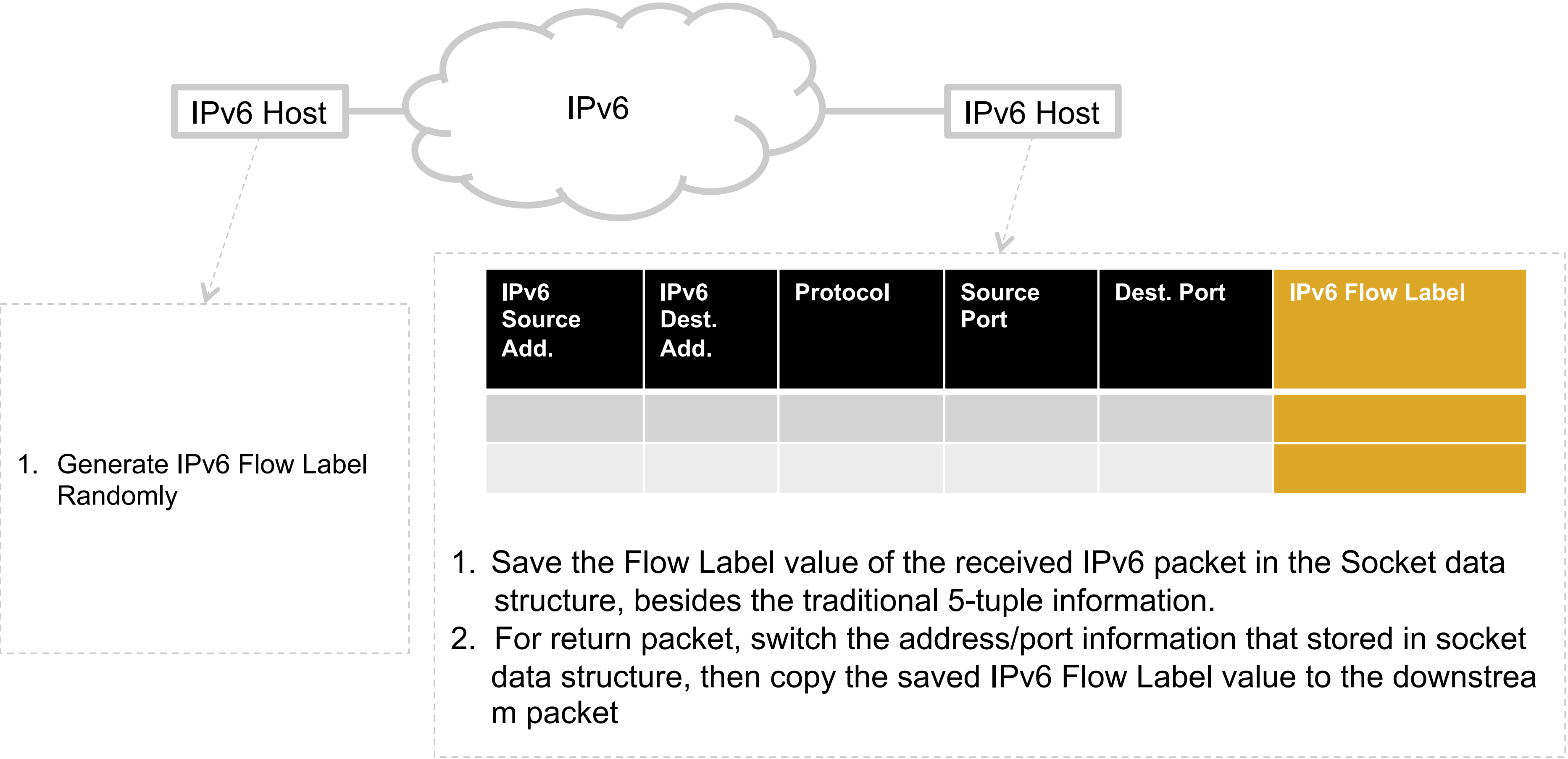
1.End to End IPv6 Communication

2.NAT64 deployed scenario

3.DS-Lite deployed scenario

Scenarios	IPv6 packet initiator	IPv6 packet terminator	Affected RFC
1. End to End IPv6 communication	IPv6 Host	IPv6 Host Action： Save the IPv6 Flow Label value in received packet， copy it to the response packet	RFC 6437
2. NAT64	IPv6 Host Action： Generate IPv6 Flow Label randomly	NAT64 Device Action： Add new column for Flow Label in NAT table of NAT64 device. Copy the saved Flow Label value to the downstream IPv6 packet.	RFC 6146
3. DS-Lite Environment	CPE Action： Generate IPv6 Flow Label randomly based on inner IPv4 5-tuple information.	AFTR Action： Add new column for Flow Label in NAT table of AFTR device. Copy the saved Flow Label value to the downstream encapsulated IPv6 packet	RFC 6333

Detail Process—End to End IPv6 Environment



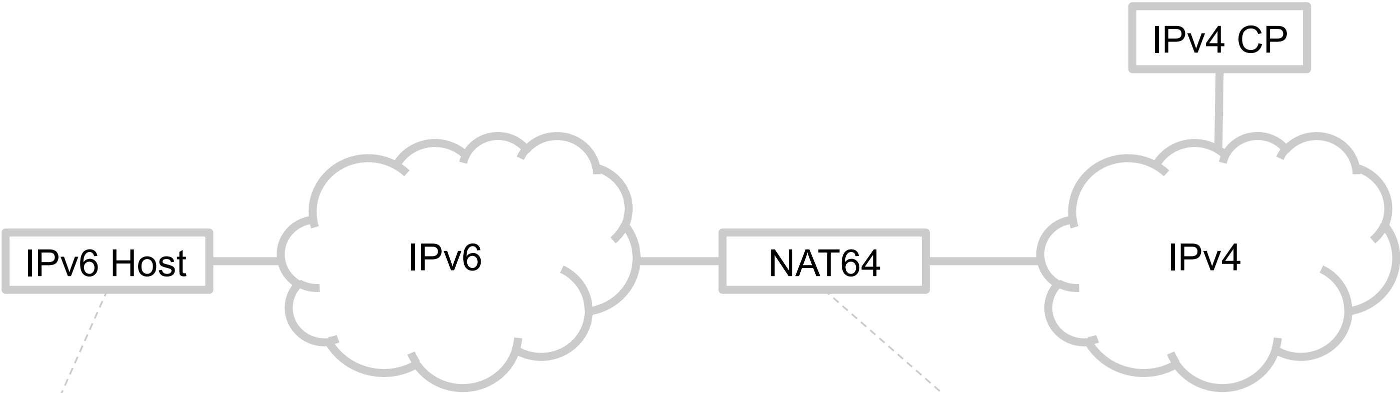
1. Generate IPv6 Flow Label Randomly

IPv6 Source Add.	IPv6 Dest. Add.	Protocol	Source Port	Dest. Port	IPv6 Flow Label

1. Save the Flow Label value of the received IPv6 packet in the Socket data structure, besides the traditional 5-tuple information.
2. For return packet, switch the address/port information that stored in socket data structure, then copy the saved IPv6 Flow Label value to the downstrea m packet

IPv6 Flow Label Reflection Mechanism in end to end IPv6 communication environment

Detail Process—NAT64 Environment



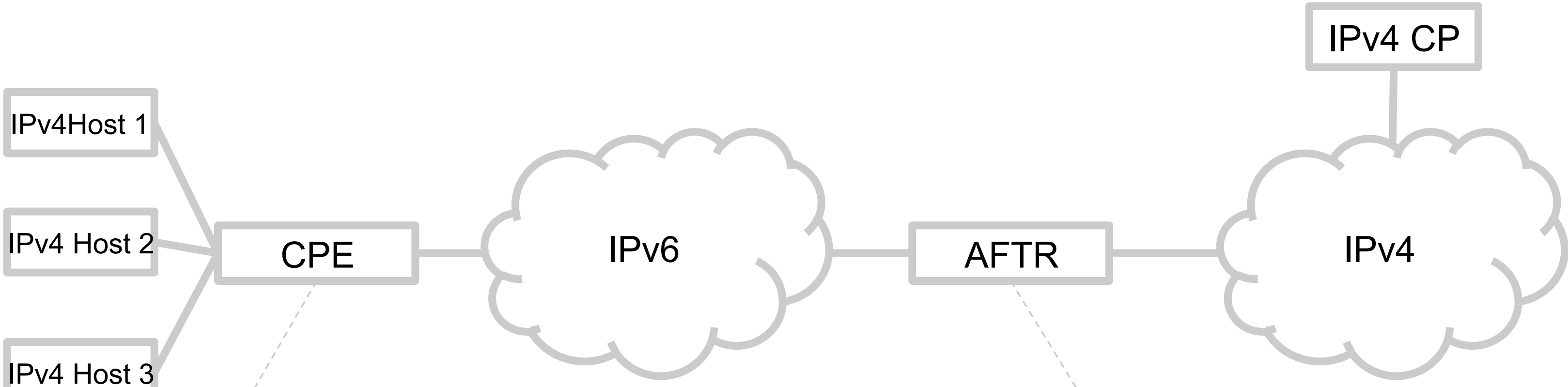
1. Generate IPv6 Flow Label randomly

IPv6 Source Add.	Synthesized IPv6 Dest Add.	Proto.	Source Port.	IPv6 Flow Label	NATed IPv4 Add.	NATed IPv4 Port.

1. Add new column in NAT table of NAT64 device, record the IPv6 Flow Label value in upstream packet
2. NAT64 device convert the downstream IPv4 packet, get the saved IPv6 Flow Label value, copy it to the downstream IPv6 packet

IPv6 Flow Label Reflection Mechanism in end to end IPv6 communication environment

Detail Process—DS-Lite Environment



1. Generate IPv6 Flow Label randomly based on the inner 5-tuple IPv4 information

IPv6 Source Add. Of CPE	IPv4 add. of IPv4 host	Proto.	Host Source. Port	IPv6 Flow Label	NATed Add. of IPv4 host	NATed Port of IPv4 host

1. Add new column in NAT table of AFTR device, record the IPv6 Flow Label value in upstream packet
2. AFTR device convert the downstream IPv4 packet, encapsulate it in IPv6 packet, get the saved IPv6 Flow Label value, copy it to the downstream encapsulated IPv6 packet

IPv6 Flow Label Reflection Mechanism in DS-Lite environment

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.

Comments, Reviews &
Contribution are appreciated!

Thanks！