IPv6 Application of the Alternate Marking Method

draft-ietf-6man-ipv6-alt-mark-01

Online, Jul 2020, IETF 108

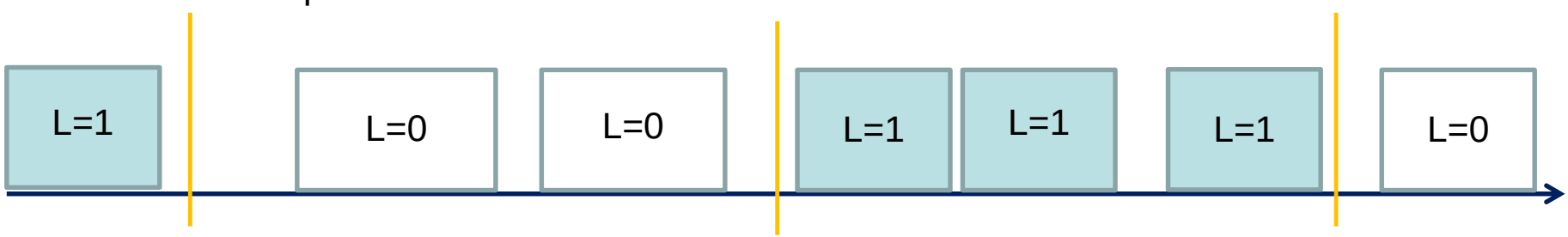
Giuseppe Fioccola (Huawei)
Tianran Zhou (Huawei)
Mauro Cociglio (Telecom Italia)
Fengwei Qin (China Mobile)
Ran Pang (China Unicom)

Alternate Marking at a glance

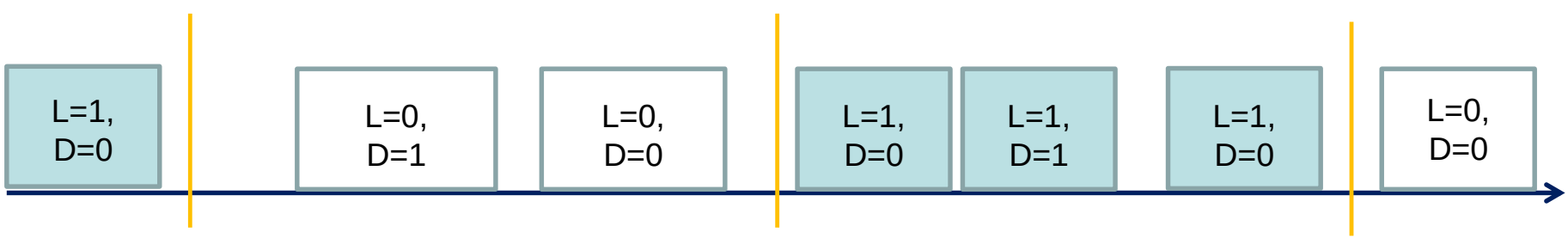
Alternate Marking methodology is an OAM PM technique and enables Packet Loss, Delay and Delay Variation measurements

The reference documents are **RFC 8321** and **draft-ietf-ippm-multipoint-alt-mark** (in RFC Editor Queue)

- Batching packets based on time interval to measure **Packet Loss** by switching value of L flag.
- **First/Last Packet Delay calculation** and **Average Packet Delay and Delay Variation** calculations are possible



- Use D flag to create a new set of marked packets fully identified over the network. D-marked packets to calculate **more informative Packet Delay Metrics**



What about IPv6 application

The main requirement for the application of the alternate marking is the **Marking Field**.

- The preferred choice is the use of the **Option Header** (Hop-by-hop or Destination)

  - ✓ The **source node** is the only one that writes the Option Header to mark alternately the flow (for both Hop-by-Hop and Destination Option).

  - ✓ **In case of Hop-by-Hop Option Header** carrying Alternate Marking bits, it is not inserted or deleted, but can be read by any node along the path. The **intermediate nodes** may be configured to read this Option or not, the measurement can be done only for the nodes configured to read the Option.

  - ✓ **In case of Destination Option Header** carrying Alternate Marking bits, it is not processed by any node until the packet reaches the **destination node**. The measurement is end-to-end.

Changes after the WG Adoption

We addressed the comments received during the adoption call from Tom Herbert and Eric Vyncke.

In particular we added:

- ✓ A new section on the Uniqueness of FlowMonID.

- ✓ Improved section on Security Considerations.

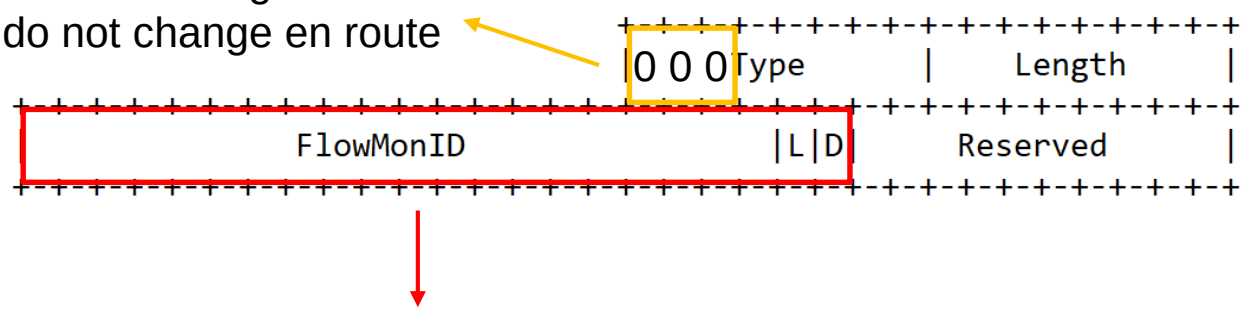
After the feedback from Ron Bonica, the next version will include:

- ✓ A paragraph about the timing aspects of the Alternate Marking and resiliency to reordering

Alternate Marking Data Fields

- Definition of a new TLV to be encoded in the Options Header
- The **AltMark Option** is expected to be encapsulated as Hop-by-Hop Options Header or Destination Options Header.

Skip if do not recognize and
data do not change en route



- **L** and **D** are the Marking Fields
- The Flow Monitoring Identification (**FlowMonID**) is required for specific deployment reasons

Flow Monitoring Identification

The Flow Monitoring Identification (**FlowMonID**) is required for some reasons:

1) **It helps to reduce the per node configuration**. Otherwise, each node needs to configure an access-control list (ACL) for each of the monitored flows. Moreover, using a flow identifier allows a flexible granularity for the flow definition.

2) **It simplifies the counters handling**. Hardware processing of flow tuples (and ACL matching) is challenging and often incurs into performance issues, especially in tunnel interfaces.

3) **It eases the data export** encapsulation and correlation for the collectors.

Uniqueness of the FlowMonID

How to allow disambiguation of the FlowMonID in case of collision.

1) In case of a **centralized controller**, it should set FlowMonID and instruct the nodes properly in order to guarantee its uniqueness.

2) FlowMonID can be **pseudo randomly generated by the source node**

- if the 20 bit FlowMonID is set independently and pseudo randomly there is a chance of collision (50% chance of collision for just 1206 flows!)
- For more entropy, FlowMonID can either be combined with other identifying flow information in a packet (e.g. IP addresses and Flow Label) or the FlowMonID size could be increased.

AltMark EH Option alternatives

In summary, here are the alternative options based on the chosen type of PM:

- ✓ **Destination Option** => measurement only by node in Destination Address.
- ✓ **Hop-by-Hop Option** => every router on the path with feature enabled.
- ✓ **Destination Option + any Routing Header** => every destination node in the route list.

In many cases the end-to-end measurement is not enough and it is required also the hop-by-hop measurement.

- Nodes that do not support the Hop-by-Hop Option SHOULD ignore them. In this case, the performance measurement does not account for all links and nodes along a path.

Security Considerations

Security concerns:

- **Harm caused by the measurement**: Alternate Marking implies modifications on the fly to an Option Header by the source node
  - This must be performed in a way that does not alter the QoS experienced by the packets and that preserves stability of routers doing the measurements.

- **Harm to the Measurement**: Alternate Marking measurements could be harmed by routers altering the marking of the packets or by an attacker injecting artificial traffic.
  - In the context of a **controlled domain**, the network nodes are locally administered and this type of attack can be avoided
  - An attacker cannot gain information about network performance from a single monitoring point but it should be able to use synchronized monitoring points to apply the method

Privacy concerns are limited because the method only relies on information contained in the Option Header without any release of user data.

  - The limited marking technique seems unlikely to substantially increase the existing privacy risks from header or encapsulation metadata.

Next Steps

- We have found an agreed way to apply RFC 8321 and draft-ietf-ippm-multipoint-alt-mark to IPv6
- IANA IPv6 Parameters: temporary assignment to test the implementation
- Welcome questions, comments

Thank you