IPv6 Application of the Alternate Marking Method

draft-ietf-6man-ipv6-alt-mark-02

Online, Nov 2020, IETF 109

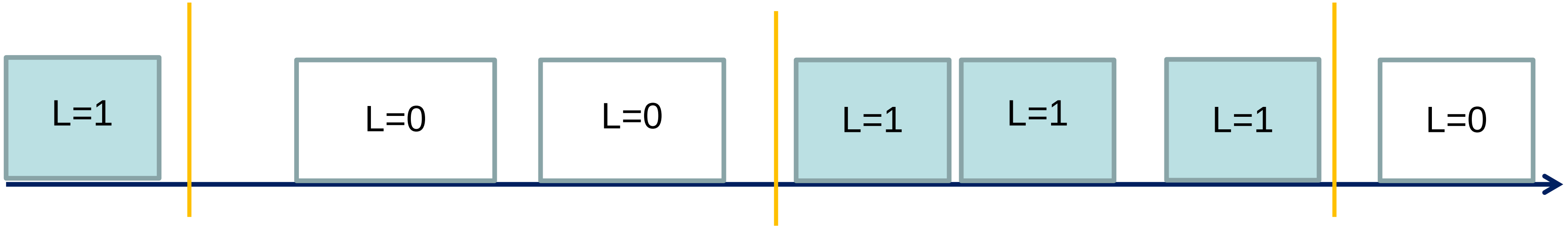
Giuseppe Fioccola (Huawei)
Tianran Zhou (Huawei)
Mauro Cociglio (Telecom Italia)
Fengwei Qin (China Mobile)
Ran Pang (China Unicom)

Alternate Marking

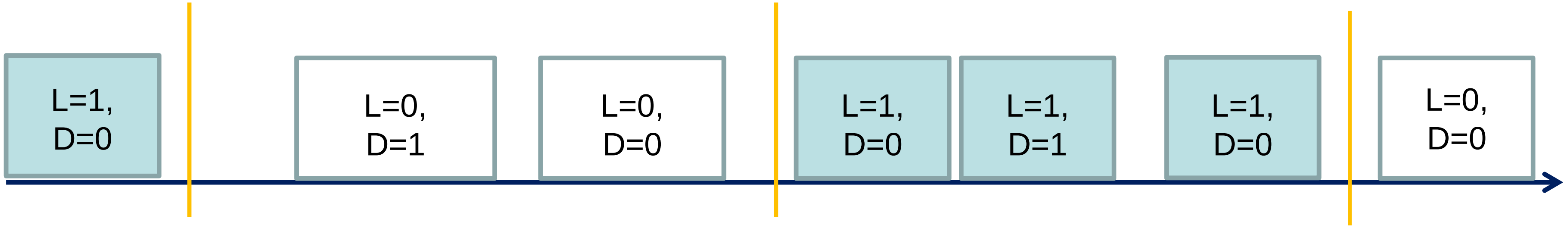
Alternate Marking methodology is an OAM PM technique and enables Packet Loss, Delay and Delay Variation measurements

The reference document is **RFC 8321**

- 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



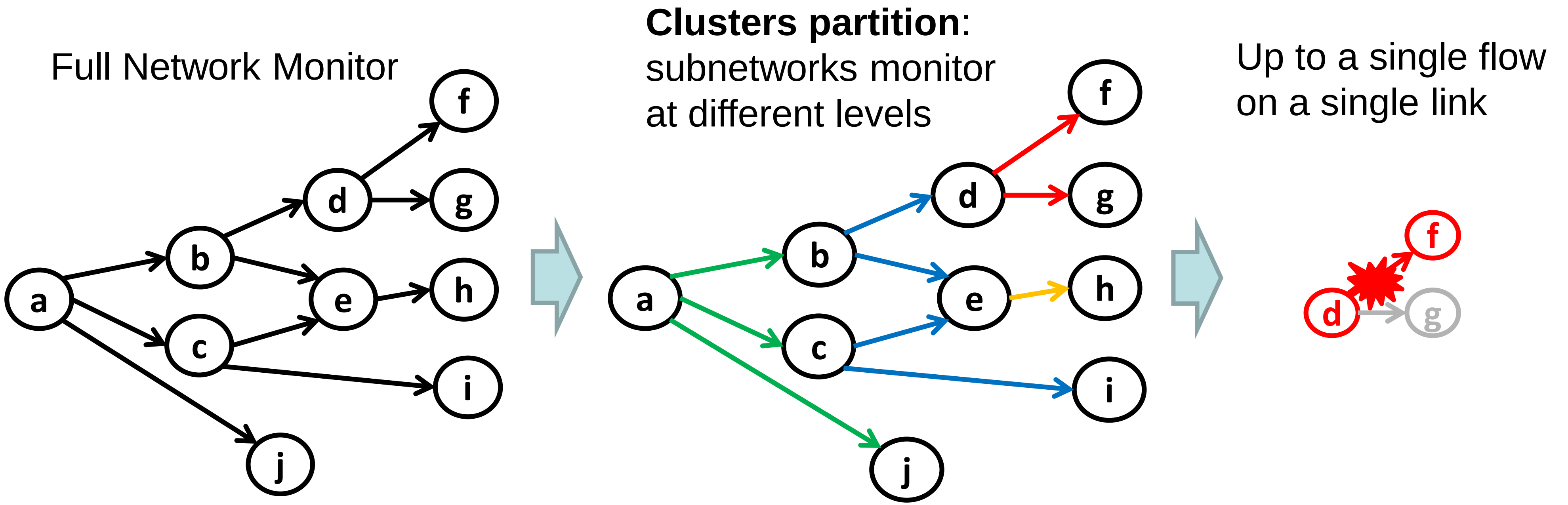
- Use D flag to create a new set of marked packets fully identified over the network. D-marked packets to calculate **more informative Packet Delay Metrics**



Multipoint Alternate Marking

Multipoint Alternate Marking methodology generalizes the application of RFC 8321 for multipoint unicast flows and allows a flexible performance management approach

The reference document is **RFC 8889**



Full Network Monitor

Clusters partition: subnetworks monitor at different levels

Up to a single flow on a single link

- **Packet Loss** can be measured on multipoint path basis (on **Cluster basis**) or considering the borderline cases of single flows and whole network.
- **Delay measurements** can be done on **multipoint path basis** or on **single packet basis** (using **RFC 5475**)

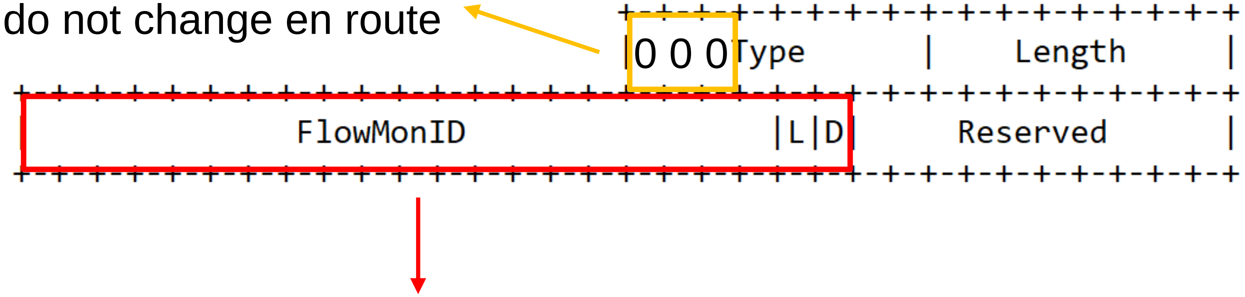
What about IPv6 application

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) carrying Alternate Marking bits
    - The **source node** is the only one that writes the Option Header to mark alternately the flow (for <u>both Hop-by-Hop and Destination Option</u>).
    - In case of **Hop-by-Hop Option Header**, it can only be read by the **intermediate nodes** along the path. The measurement can be hop-by-hop but it is done only for the nodes configured to read the Option.
    - In case of **Destination Option Header**, it is not processed by any node until the packet reaches the **destination node**. The measurement is end-to-end.

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

```
                                +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                |0 0 0Type      |     Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              FlowMonID                |L|D|     Reserved       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

Flow Monitoring Identification

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

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

- ✓ **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.

- ✓ **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 could be required the hop-by-hop measurement.

- Nodes that do not support the Hop-by-Hop Option SHOULD ignore them. In this case, the 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 multiple and 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.

Changes from -01 to -02

Inputs during IETF 108:

Revision from Ron Bonica, thus we have included:

- ✓ A paragraph about the timing aspects of the Alternate Marking and resiliency to reordering
- ✓ The detailed formulations are described in RFC8321 and RFC8889

Comment from Igor Lubashev

It could be possible to pick up one of the bits in the Reserved field for cross-layer telemetry information (e.g. QUIC/TCP Measurements)

- ▪ Anyway this is out of scope for now and it could be evaluated in a future extension

Next Steps

- An agreed way to apply RFC 8321 and RFC 8889 to IPv6 has been found
- IANA IPv6 Parameters assignment to test the implementation
- Welcome questions, comments

Thank you