IPv6 Application of the Alternate Marking Method

draft-ietf-6man-ipv6-alt-mark-12

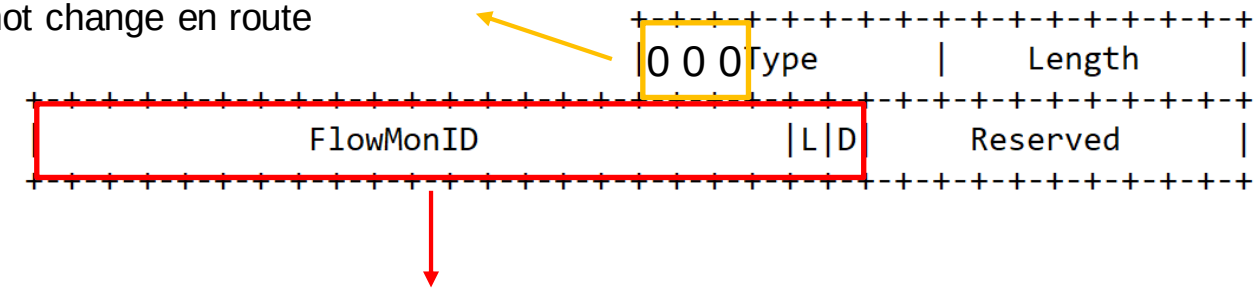
Online, Nov 2021, IETF 112

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

IPv6 Alternate Marking Option

- 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 (see next slide)

- 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**, it can only be read by the **intermediate nodes** along the path. The measurement is hop-by-hop.
- 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.

IESG Evaluation
Summary of the Changes

Section on Controlled Domain has been improved

- The precondition for AltMark application explained

New subsection on Alternate Marking Measurement Domain

- Usage scenarios of the measurement domain have been clarified

Specification of Flow Monitoring Identification

- FlowMonID to be used in combination with source and destination addresses

Security section revised

- Additional considerations added

Controlled Domain and Measurement Domain

The IPv6 application of the Alternate Marking Method MUST be deployed in a controlled domain.

It is RECOMMENDED that an implementation filters packets that carry AltMark data and are entering or leaving the controlled domains.

The Alternate Marking measurement domain can overlap with the controlled domain or may be a subset of the controlled domain.

The typical scenarios are now clarified:

- the **UE** can be the starting or ending node, only in case it is fully managed and if it belongs to the controlled domain. But, this is not common because the UE could not be totally secured.
- the **CPE** is most likely to be the starting or ending node since it connects the user's premises with the operator's controlled domain. Typically the CPE encapsulates a received packet in an outer IPv6 header which contains the AltMark data.
    - The CPE can also be able to filter and drop packets to make effective the relevant security rules at the domain boundaries.

Flow Monitoring Identification

The FlowMonID MUST only be used as a monitored flow identifier in order to determine a monitored flow within the measurement domain.

Since there is a chance of collision, it is RECOMMENDED to use the FlowMonID for identification purpose in combination with source and destination addresses to identify a flow

- If the 20 bit FlowMonID is set independently and pseudo randomly in a distributed way, there is a 50% chance of collision for 1206 flows.
  - It is possible to monitor 145 concurrent flows per host pairs with a 1% chance of collision.

- If the 20 bit FlowMonID is set in a centralized way, the controller can instruct the nodes properly. With 20 bits, the number of combinations is 1048576, and the controller should ensure that all the FlowMonID values are used.
  - It can be possible to monitor 1048576 concurrent flows per host pairs.

All the nodes along the path and involved into the measurement SHOULD use the same mode for identification.

Security Considerations

The precondition for the Alternate Marking is the application to controlled domains, thus mitigating and confining the potential attack vectors. New considerations added:

- Network nodes can intentionally alter the bits of the AltMark Option or inject Options headers as a means for DoS. The implementation of the method is done on managed nodes.

- Packets generated outside the controlled domain may consume router resources by maliciously using the HbH Option, but this can be mitigated by filtering these packets at domain boundaries.

- AltMark Option metadata can be used for network reconnaissance to compromise the privacy of users. The FlowMonID is a sensitive information if it goes outside the controlled domain.

- Leakages may happen, such as a failure or a fault. In this case, nodes outside the domain MUST simply ignore packets with AltMark Option since they should not process it.

- The specific deployment scenario (Hop-by-Hop or Destination Option) can involve multiple administrative domains traversed by the AltMark. To this end, the inter-domain links need to be secured (e.g., by IPsec, VPNs) in order to realize the whole controlled domain.

- It might be theoretically possible to modulate the marking or the other fields to serve as a covert channel to be used by an on-path observer. Controlled domain application helps here.

Summary and Next Steps

- A pending point is the informative reference to experimental RFC8321 and RFC8889

- Welcome questions, comments

Thank you