Alternate Marking Deployment Framework

draft-fz-ippm-alt-mark-deployment-01

Prague, Nov 2023, IETF 118

Giuseppe Fioccola
Tianran Zhou
Keyi Zhu
Huawei

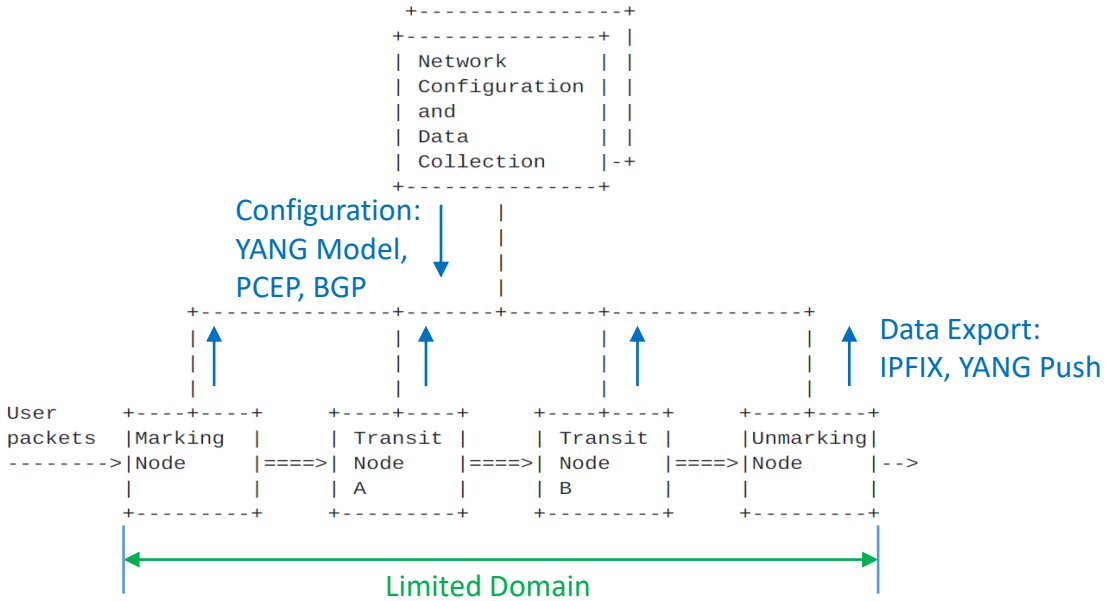
Thomas Graf
Swisscom

Fabrizio Milan
Massimo Nilo
Telecom Italia

Lin Zhang
China Mobile

Background and Motivation

- RFC 9341, RFC 9342 and RFC9343 have been published last year.
- This draft aims to provide guidance for the AltMark deployment, especially with regard to the manageability



The draft aims to clarify the following aspects:

- AltMark Deployment Domain
- AltMark Measurement Nodes
- Type of Measurements
- Operational Guidelines
- Manageability and Configuration Aspects
- Data Export, Collection and Calculation
- Encapsulations
- Security

AltMark Deployment Domain, Measurement Nodes, Type of Measurements and Operational Guidelines

AltMark Deployment Domain and Measurement Nodes
The Alternate Marking Method is deployed in a **controlled domain** for security and compatibility reasons (see RFC 8799)

- The typical **deployment domain** is an overlay network, where traffic is encapsulated at one domain border, decapsulated at the other domain border and the encapsulation incorporates the extension header for Alternate Marking.

An Alternate-Marking Domain consists of **marking nodes**, **unmarking nodes**, and **transit nodes**.

Type of Measurements
Either one or two flag bits might be available for marking in different deployments:

- **One flag**: packet loss measurement as described in Section 3.1 of RFC9341, while delay measurement according to the single-marking method described in Section 3.2.1 of RFC9341. Mean delay (Section 3.2.1.1 of RFC9341) could also be used
- **Two flags**: packet loss measurement as described in Section 3.1 of RFC9341, while delay measurement according to double-marking method Section 3.2.2 of RFC9341.

Operational Guidelines
Considerations on the kind of information that can be derived, the measurement frequency, the computational load,…

Configuration Aspects, Data Export, Collection and Calculation, Encapsulations and Security

Configuration
The YANG model can be used for the definition of the AltMark data sent over network management protocols such as the NETCONF and RESTCONF.

- draft-gfz-ippm-alt-mark-yang has been proposed

There are also other control plane mechanisms to advertise and activate AltMark capabilities, using PCEP or BGP:

- draft-ietf-idr-sr-policy-ifit, draft-ietf-idr-bgp-ifit-capabilities, draft-ietf-pce-pcep-ifit

Data Export
The new IPFIX Information Elements (IEs) to export Alternate Marking measurement data are specified in draft-gfz-opsawg-ipfix-alt-mark.

- In addition to IPFIX, YANG Push can also be used
- Packet counts and timestamps are reported to the collector, but a certain synchronization mechanism is required to ensure that the collected data is correlated.
    - the Period Number can be used to help to determine the packet counts related to the same block of markers, or the timestamps related to the same marked packet.

Encapsulations and Security
Different Encapsulations have been reported (IPv6, SRv6, BIER, MPLS, SFC, NVO3,…) and the Security fundamental requirement of the limited domain is also highlighted (RFC8799).

Changes from -00

Received comments from Chongfeng Xie, Greg Mirsky, Thomas Graf and Massimo Nilo.

- New section on Configuration
- Revised section on Data Export
  - IPFIX and YANG Push (Thanks to Thomas Graf)

- New Section on Implementation Observations

Next Steps

Evaluate WG Adoption

Comments are welcome!

Thank You