

Network Working Group
Internet-Draft
Intended status: Experimental
Expires: April 27, 2022

Z. Du
P. Liu
China Mobile
October 24, 2021

Self-Contained Alternate-Marking Mechanism for Performance Monitoring in
High-Quality Network
draft-du-ippm-self-contained-alt-mark-00

Abstract

This document introduces a self-contained method that can involve the client in based on some extensions to the alternate-marking (coloring) technique.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 27, 2022.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Traditional Mechanism Description	3
3. Proposed Mechanism Description	4
4. Analysis of the Potential Problems	5
5. IANA Considerations	5
6. Security Considerations	5
7. Acknowledgements	5
8. References	5
8.1. Normative References	6
8.2. Informative References	6
Authors' Addresses	6

1. Introduction

The network operators are planning to provide network services with higher quality than the traditional BE (Best Effort) service, such as the DetNet service [RFC8655] and the Network Slicing service. In these practices, it is important to monitor the performance of the service, such as the packet loss, delay, and jitter of the flow with guaranteed quality.

In [RFC8321], an alternate-marking method for passive and hybrid performance monitoring is proposed. It marks the packet by using one or more bits in the packet headers, and collects the number of packets in a block sent on one end and the number of packets in the same block received on the other end. Finally, the two values are compared and accordingly, the packet loss of the flow are computed.

The alternate-marking method is potential applied to any kind of packet-based traffic, and easy to implement. However, a controller or NMS needs to collect the information from the coloring point and the monitoring point, and correlate the two pieces of information by using the same block ID. It is hard to make it an end-to-end solution because the client is not in the scope.

In this document, we propose a method that can involve the client in based on some extensions to the alternate-marking (coloring) technique. In this method, the block information is serialized and encoded in the packets of the block by the client. Then, the monitoring points can recover the information from the received

packets, such as the block ID, number of packets in the block, timestamps in the packet, and compute the target measurement values.

2. Traditional Mechanism Description

As described in [RFC8321], the alternate-marking method is based on the "block", which represents a measurable entity unambiguously recognizable by all network devices along the path.

In the alternate-marking (coloring) technique, the coloring point creates packet blocks, colors the packets in the block, and reports information including block ID to the controller or the NMS. The monitoring points recognize the coloring information, record some needed information and report it to the controller or the NMS.

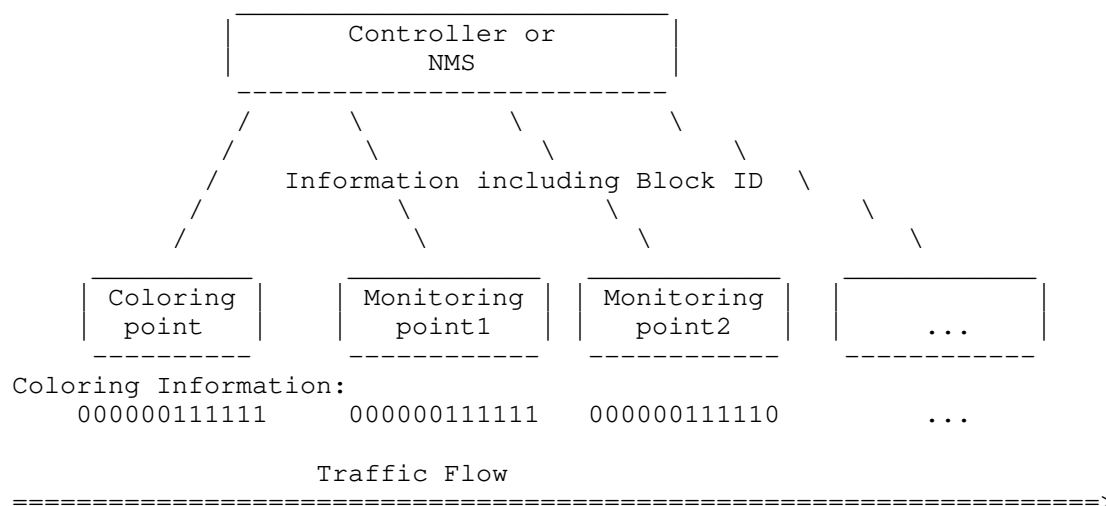


Figure 1: Mechanism in the traditional alternate-marking method

For example, if some packets are lost in the network, the packet numbers of the same block will be different between the coloring point and the monitoring point. If we need to compute the delay or jitter of the flow, the coloring point and the monitoring point can also report the timestamps of the packets in the block to the controller or NMS.

Traffic coloring can be implemented by setting a specific bit in the packet header and changing the value of that bit periodically. Thus, we only need two colors, and the packets belonging to the same block

have the same color, whilst consecutive blocks will have different colors.

When the color changes, the previous block terminates and the new one begins. Two mechanisms of switching color are introduced in [RFC8321]. The first one is to switch the color after a fixed number of packets. The second one is to switch according to a fixed timer. For example, the timer may be 5 minutes.

3. Proposed Mechanism Description

To make the block information self-contained in the block, we need to occupy another specific bit to encode the block information. Thus, the client in the proposed mechanism needs not to report anything to the controller or NMS, and the monitoring points can compute target measurement values themselves and report any problem if needed.

For example, we assume the fixed timer mechanism is used, and there are about 300 packets in a block. In the client, each packet carries one bit of the block information. Thus, if all the packets are received orderly, a monitoring point can recover the block information encoded in those 300 packets.

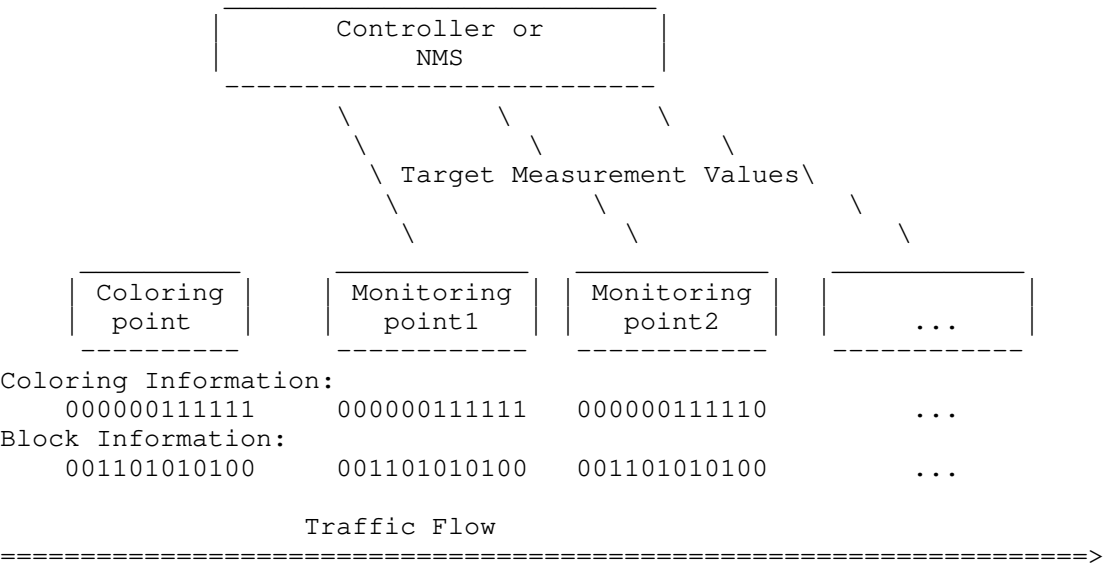


Figure 2: Mechanism in the self-contained alternate-marking method

The block information can include the block ID (32 bits), CRC (32bits), and some TLVs as described below.

- o TLV 1 may be the interval of the block (32bits).
- o TLV 2 may be the packet number of the last block (32bits).
- o TLV 3 may be the timestamp of the first packet in the block (32bits).

The encoding of the block information is done in the client, and the monitoring points need to understand the meaning of the encoding.

4. Analysis of the Potential Problems

As described in the last section, we assume that all the packets in a block are received in the monitoring point orderly. Normally, it is hard for the IP network with a relatively high packet loss rate. However, the situation may be much better in the DetNet service or the Network Slicing service, for which no or few packets would be lost. Meanwhile, an additional recovery block may also appear after several blocks, in which we will encode recovery information for the past several blocks, instead of the block information. Other fault tolerance mechanisms can also be considered.

Another problem is similar to the situation in [RFC8321]. It is whether we can find at least two reserved bits in the packet header to encode the coloring information and the block information. The detailed analysis can be found in that document.

5. IANA Considerations

TBD.

6. Security Considerations

TBD.

7. Acknowledgements

TBD.

8. References

8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC8321] Fioccola, G., Ed., Capello, A., Cociglio, M., Castaldelli, L., Chen, M., Zheng, L., Mirsky, G., and T. Mizrahi, "Alternate-Marking Method for Passive and Hybrid Performance Monitoring", RFC 8321, DOI 10.17487/RFC8321, January 2018, <<https://www.rfc-editor.org/info/rfc8321>>.

8.2. Informative References

- [RFC8655] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <<https://www.rfc-editor.org/info/rfc8655>>.

Authors' Addresses

Zongpeng Du
China Mobile
No.32 XuanWuMen West Street
Beijing 100053
China

Email: duzongpeng@foxmail.com

Peng Liu
China Mobile
No.32 XuanWuMen West Street
Beijing 100053
China

Email: liupengyjy@chinamobile.com