Workgroup: IPPM
Internet-Draft:
draft-li-ippm-ioam-path-protection-01
Published: 11 July 2022
Intended Status: Experimental
Expires: 12 January 2023
Authors: Z.LI. Li, Ed.
CAICT

IOAM Linkage Solution for the Protection Cases of 5G Bearer Network

Abstract

In-band operation and maintenance management (IOAM, In-band OAM), as a network performance monitoring technology, is based on the principle of path-associated detection to perform specific field marking/coloring and identification on actual service flows, and perform packet loss and delay measurement. It can quickly perceive network performance-related faults, and accurately delimit boundaries and do troubleshooting. However, the current IOAM solution has shortcomings too. For example, after the service traffic path switching, the IOAM cannot continue working. This paper proposes a scheme to achieve automatic performance monitoring through service path switching and linkage with IOAM, which enhances the feasibility of the IOAM scheme in large-scale deployment and the completeness of IOAM technology.

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 12 January 2023.

Copyright Notice

Copyright (c) 2022 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction
  1.1. Requirements Language
  1.2. Terminology
2. IOAM basic processing analysis
3. The impact of service path switching on IOAM
  3.1. Analysis of Service Protection Mechanism
  3.2. The impact of service path switching on IOAM
  3.3. Summary
4. IOAM monitoring is associated with service path
  4.1. Key points of the linkage solution
    4.1.1. Service path changes notice IOAM module
    4.1.2. Reconfigure mechanism
  4.2. The process of the linkage solution
5. Acknowledgements
6. IANA Considerations
7. Security Considerations
8. References
  8.1. Normative References
  8.2. Informative References
Author's Address

1. Introduction

In-band operation and maintenance management (In-band OAM, IOAM) is a flow monitoring technology with high accuracy. It does not need to use out-of-band monitoring messages, and measures network KPIs such as packet loss and delay directly. But there are also shortcomings: in the current solution, performance monitoring can only be performed based on traffic quintuple information (pre-configuration or learning from traffic flow). If the path of this flow changes, it cannot working in most cases. However, In real network , the service flow path is not stable. There are many reasons for the change of the flow path, such as the interruption of the working fiber link in the network and the error code exceeding the threshold, or switching traffic to the backup link temporarily because of the equipments' upgrade. Regardless of the cause of the service traffic path switching, it is of great significance to monitor the performance on

the new path after the switching automatically. Service path switching is a key event in the network. If the switched service path is not monitored in real time, it is impossible to ensure that the switched path can meet the requirements of the upper-layer service; on the contrary, if the IOAM performance monitoring of the switched path can be used to detect the deterioration of the network KPI after the switch in time , the operator may optimize and adjust the service path as soon as possible. Except for the manual and planned switching, it is difficult to predict the time for other switching caused by network failures, which will also cause the network operator to be unable to redeploy and start IOAM performance monitoring in time after the switching.

1.1. 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].

1.2. Terminology

IOAM:In-band Operation And Maintenance Management

KPI:Key Performance Indicator

HSB:Hot Standby

APS:Automatic Protect Switch

Ti-LFA:Topology Independent Loop Free Alternate

SD:Signal Degrade

UNI:User Network Interface

NNI:Network Network Interface

2. IOAM basic processing analysis

IOAM Data collection and analysis process is shown in the figure1:

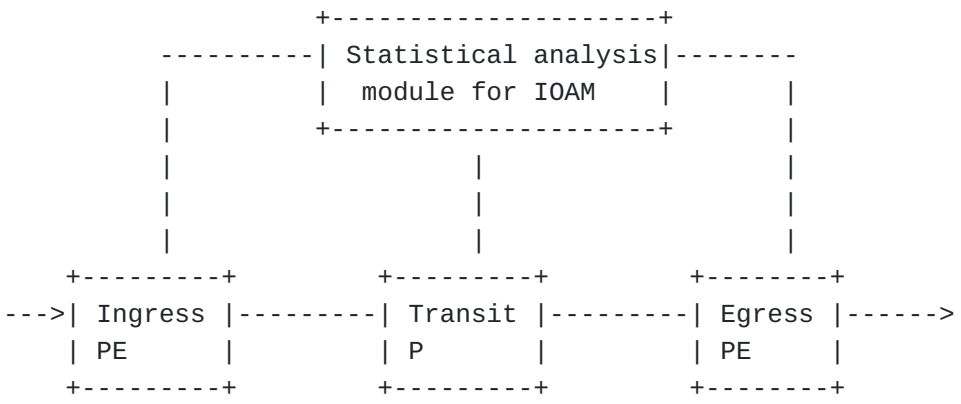


Figure 1

IOAM Data collection and analysis process

*At the ingress PE, the UNI side uses ACL to match the quintuple information of the service flow, dyes the matched traffic packets and sends the statistics to the statistical analysis module in the network controller. The NNI side encapsulates the IOAM header and service label (SR-TE/SR-BE and VPN label);

*The P device reads the IOAM header information (Flow ID and colored bit information). The IOAM header is inside the SR label and the VPN label, and there is no need to decapsulate and recapsulate it to avoid too much impact on the forwarding performance; this step only involves hop-by-hop monitoring, not end-to-end monitoring.

*At the egress PE, decapsulate the packet, read the information in the IOAM header, report to the statistical analysis module, and then send the original user payload from the UNI side;

*The statistical analysis module combines the topology information to perform statistical analysis on the data sent by the network equipments, and present it through reports or graphics.

3. The impact of service path switching on IOAM

3.1. Analysis of Service Protection Mechanism

If it is an automatic switching triggered by a network failure, it can be divided into signal failure (SF, often caused by line fiber break, equipment power failure), signal degradation (SD, line error or packet loss over the threshold of performance availability, due to aging of fiber. Switching occurs when the error rate or the accumulated packet loss rate reaches the detection threshold). Fiber breakage, power failure of P node, and SD error codes will trigger HSB or APS switching (for SR-TE tunnel) or Ti-LFA protection (for

SR-BE tunnel), the tail node power failure will trigger VPN FRR(Fast reroute) protection.

If the switching is triggered because of network expansion, upgrade, etc., the switching mechanism is basically the same as the network failure trigger, and the impact on IOAM is also the same, so it will not be analyzed separately.

3.2. The impact of service path switching on IOAM

As shown in Figure2 below, network equipments A, C, and G are PE devices; B ,E and F are P devices, and D is CE devices. Under normal condition, services are forwarded through the working tunnel path, which is A-B-C-D ; The protection tunnel path is A-E-F-G-C-D (one by one protection path of the tunnel), and the tail node protection path is A-E-F-G-D.

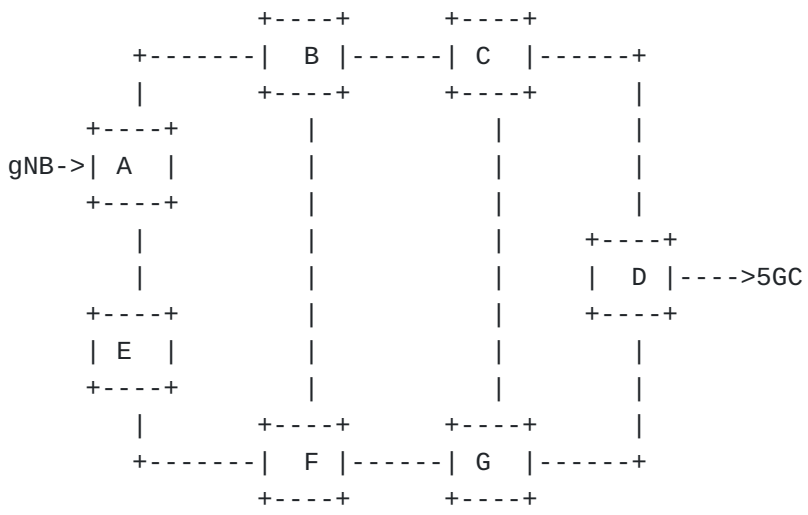


Figure 2

5G Bearer Network with Backup Path

1. When the working path is normal, configure IOAM end-to-end instances on A and C respectively, or configure IOAM hop-by-hop instances on A, B, and C to monitor the delay and packet loss.

2. Taking the L3VPN over SR-TE tunnel as an example, when the Node B or the link between A and C fails, the HSB protection of the SR-TE tunnel is triggered, and the service traffic switchs to A-E-F-G-C-G, the end-to-end IOAM monitoring is not affected; because Node B fails , the hop-by-hop monitoring instance cannot continue to obtain the data reported by B, so the relevant configuration of the monitoring instance needs to be switched to each node of the backup path, that is, the IOAM

monitoring instance needs to be newly configured at node E, F, and G.

3. When the node C fails, the VPN FRR protection is triggered. Because the PE is switched to node G, the end-to-end and the hop by hop monitoring instance will become invalid, and it is impossible to continue to monitor the KPI of the service on the protection path. IOAM monitoring needs to be newly configured at nodes E, F, and G.

4. The statistical analysis module in the network controller combines the topology information to perform statistical analysis on the data sent by the network equipments, and present it through reports or graphics.

3.3. Summary

From the above, it can be seen that the change in the flow direction caused by the switching of the active and standby service paths will directly affect the data collection and reporting of the IOAM monitoring instance. Based on the existing solution, one way to continue monitoring after the switch is to deploy IOAM monitoring on all nodes of the active and standby paths. When there is no traffic on the standby path, the nodes along the way do not report monitoring data; whenever traffic reaches, the monitoring data will be reported again. There are two issues with this solution: the first one is that after the traffic is switched, because there is no linkage, the upper-layer statistical analysis module in the controller does not perceive the change of the service path, and does not know what the real service path is, so it may not be able to calculate the result of delay and packet loss normally; the second one is that it will cause waste of IOAM resources configured on the device that no traffic passes through. Therefore, if a certain linkage mechanism can be established between the IOAM and the service path to dynamically perceive this path change, and reconfigure in time, continuous IOAM monitoring will be performed automatically when the service path switches and recovers(except a short interruption during the switching process), and no additional IOAM resources are occupied.

4. IOAM monitoring is associated with service path

4.1. Key points of the linkage solution

4.1.1. Service path changes notice IOAM module

When the service path changes, the IOAM management module in the network controller can be notified through the alarms or events reported by the device; in addition, after the IGP on the device detects the network topology change, it will also notify network

controller to perform the topology refresh through the BGP-LS protocol.

4.1.2. Reconfigure mechanism

a. Identify the equipment that needs to be configured:according to the principle that the UNI interface on the access side(node A,connect to gNB) will remain unchanged and the corresponding relationship between the UNI interface -> VPN instance -> SR-TE/SR-BE tunnel index, the corresponding tunnel path can be queried, and then the node that needs to reconfigure the IOAM instance can be determined; The UNI interface on the core side(node C and G,connect to 5GC) may change due to the power failure or recovery of the PE device(node C), so the nodes of the IOAM instance in the downstream direction(5GC to gNB) cannot be queried in the same way as in the upstream direction(gNB to 5GC), so how to get the tunnel path and nodes in this direcion will be considered later,and updated in new version of this draft. For nodes that already have IOAM configuration, reconfiguration will not cause problems.

b. Information and sources to be configured, as shown below:

   *IOAM instance:End-to-end or hop-by-hop, unchanged before and after switching

   *Node type:PE or P, determined according to the tunnel path information, the source and tail nodes are PE, and the others are P

   *Flow ID:The same before and after the switching

   *Stream quintuple:The same before and after switching

   *UNI interface and VLAN on the access side:The same before and after switching

   *UNI interface and VLAN on the core side:To be disscussed in new version of draft

   *Telemetry configuration:Relatively fixed, generated by the controller

c. Configuration protocol:Use Netconf protocol for configuration delivery.

4.2. The process of the linkage solution

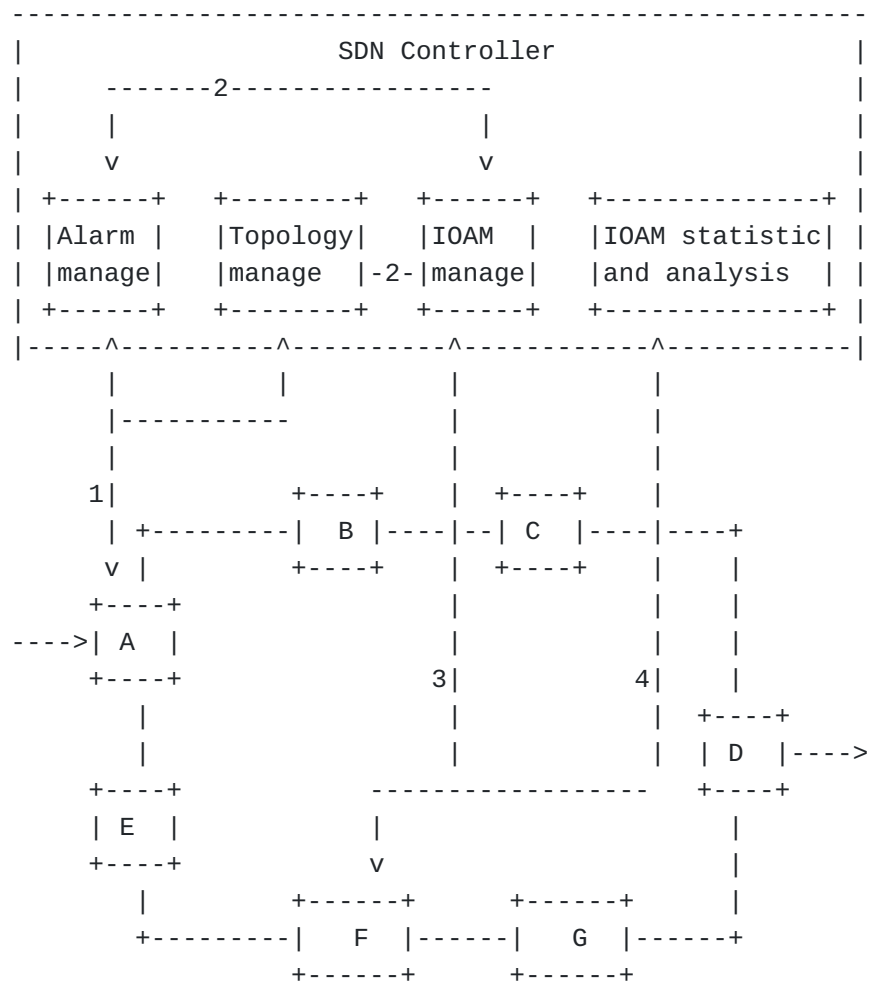


Figure 3

Process of IOAM and service path linkage scheme

1. For link or node failure, perform the corresponding fast switching (HSB/VPN FRR or Ti-LFA), and generate an alarm and send it to the network controller. IGP also detects the topology changes and reports to the controller through BGP-LS.

2. Alarm management module and topology management module in the network controller notify the IOAM management module after receiving the fast switching trigger event or alarm sent by devices, or after the BGP-LS topology is refreshed.

3. The IOAM management module queries the tunnel path information after the switching, and determines the node that needs to reconfigure IOAM and the required information according to the method in section 2) above: "Reconfigure mechanism", and perform configuration provision.

4. The IOAM management module starts the monitoring instance, the device reports the collected data with Telemetry, and the IOAM statistical analysis module analyzes and presents the monitoring results.

5. When the network failure recovers, the controller notifies the IOAM management module to reconfigure according to the received switching recovery event or BGP-LS topology refresh.

6. After the configuration of the IOAM management module is completed, the monitoring instance is started, and the monitoring results based on the restored path are presented.

5. Acknowledgements

TBD

6. IANA Considerations

This memo includes no request to IANA.

7. Security Considerations

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>.

8.2. Informative References

[RFC8321] G.Fioccola, "Alternate-Marking Method for Passive and Hybrid Performance Monitoring.", 2018, <https://datatracker.ietf.org/doc/rfc8321/>.

[YDT38262021] CCSA, "General Technical Requirements for Slicing Packet Network(SPN).", 2021.

Author's Address

Zhenwen Li (editor)
CAICT
Beijing
China

Email: lizhenwen@caict.ac.cn