Workgroup: OPSAWG Working Group
Internet-Draft:
draft-hwy-opsawg-ifl-framework-00
Published: 3 March 2022
Intended Status: Informational
Expires: 4 September 2022

Authors: L. Han M. Wang F. Yang
China Mobile China Mobile Huawei Technologies

Inband Flow Learning Framework

Abstract

To deploy the inband performance measurement and flow information telemetry on live traffic, this document proposes a framework of an inband and flow based flow information learning mechanism called Inband Flow Learning (IFL). This document also provides different deployment approaches and considerations in practical network deployment.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Network telemetry [I-D.ietf-opsawg-ntf] is a technology for gaining network insight by applying means of network data generation, data collection, data correlation, and data consumption. It provides the network visibility to the state and behavior of a network, which is crucial for network operation and network load supervision. From operator's perspective, it is important to monitor live traffic running in the network, including the bandwidth occupied by the traffic, traffic delay, traffic jitter and traffic packet loss. Under this circumstance, inband performance measurement [I-D.ietf-mpls-inband-pm-encapsulation] [I-D.ietf-6man-ipv6-alt-mark] and inband flow information telemetry [I-D.song-opsawg-ifit-framework] work complementary to provide the network traffic supervision.

To deploy the inband performance measurement and flow information telemetry on live traffic, this document proposes a framework of an inband and flow based flow information learning mechanism called Inband Flow Learning (IFL). This document also provides different deployment approaches and considerations in practical network deployment. Note that this document focuses on generating telemetry data object based on inband performance measurement of data packet. Telemetry based on means other than inband performance measurement of data packet is not within the scope of this document.

2. Terminology

IFL: Inband Flow Learning

IFITI: Inband Flow Information Telemetry Instance

3. Framework of Inband Flow Learning

The framework of Inband Flow Learning (IFL) includes three components of Service Discovery, Inband Flow Information Telemetry Deployment and Inband Flow Information Telemetry Adjustment shown in Figure 1.

Component	Service Discovery	Inband Flow Information Telemetry Deployment	Inband Flow Information Telemetry Adjus
Function	Flow characteristic acquisition	Telemetry type Telemetry policy Telemetry instance	Telemetry inst aging
Means	Configuration trigger	Controller Deploy	Data plane tri
	Live traffic sampling	Device Deploy	Controller tri

Figure 1 Framework of Inband Flow Learning

Service Discovery: before starting the telemetry on service flows, characteristics of traffic which is currently being forwarded in network should be analyzed. The traffic characteristics can be acquired either from network operations or automatically generated from the sampling of live traffics.

Inband Flow Information Telemetry Deployment: after acquiring the traffic characteristics, telemetry of service flows can be planned and deployed. In IFL, telemetry is based on a class of flow characteristic and managed as an Inband Flow Information Telemetry Instance (IFITI). Before the network node starts the telemetry, the IFITI type and policy should be specified.

Inband Flow Information Telemetry Adjustment: when the traffic changes, telemetry instance varies as well. This components includes the identification of traffic change and further adjustment of telemetry instances.

4. Service Discovery

Service discovery is a process of sampling to the service flow which is being transmitted in network in order to further determine which flow should be monitored. The characteristics of service flow are represented as IP source address, IP destination address, TCP/UDP port number, VRF, incoming/outgoing interface on network node, etc. To target of service discovery is to obtain the flow characteristics. There are two fundamental means to acquire the flow characteristics including configuration triggered and sampling based on live traffics. Regarding the means of triggered by configuration, not only includes the configuration of Interface/IP address/VRF/ Route... configured on the network nodes, but also database of planed service flow information stored on the controller and obtained from network operations, such as a table of services between base station and core network elements. On the other hand, sampling on the live traffic means that the network node automatically samples the live traffic in network, and dynamically generate flow characteristics based on live traffic. It relies on the capability of forwarding plane of network node. The comparison of two means are provided in Figure 2.

Means	Configuration trigger	Live traffic sampling
pros	Easy	real time
cons	miss of exceptions	extra FP capability required

Figure 2 Comparison of Means of Service Discovery

5. Inband Flow Information Telemetry Deployment

5.1. Telemetry Type

Inband flow information telemetry can be categorized into two modes: End-to-End (E2E) and Hop-by-Hop (HbH). For majority of services, E2E telemetry of service flows can meet the requirements from operators. In E2E mode shown in Figure 3, ingress node discovers the traffic characteristics and proceed on-path telemetry on device to report data to data consumer. Ingress node may also encapsulate flow identifier to facilitate the identification of flow information telemetry on egress node. Egress node identifies the flow and alternate marking identifier, proceed the record on packet number and timestamp, and further telemetry the statistics to data consumer. Transit node does not require any detection of flow information or processing of telemetry.

```
                        +-------------+
                        |Data Consumer| compute E2E flow info
                        +-------------+
                           |        |
             ___flow info__|        |____flow info____
            |   telemetry                telemetry    |
            |                                         |
     +---------+   +---------+    +---------+   +---------+
     | Ingress |---| Transit | ...| Transit |---| Egress  |
     |   Node  |   |   Node  |    |   Node  |   |   Node  |
     +---------+   +---------+    +---------+   +---------+
```

Figure 3 End-to-End Telemetry Type Mode

The distinction of HbH mode to E2E mode is that transit node also participates the inband flow information learning and telemetry. In HbH mode shown in Figure 4, telemetry covers the flow information on every node of the forwarding path the flow packet is transmitted, which provides detailed flow information on each hop.

```
                       +-------------+
                       |Data Consumer| compute HbH flow info
                       +-------------+
                          |   |  |   |  flow info telemetry
           _______________|   |  |   |_________________
          |                ___|  |___                  |
          |               |          |                 |
      +---------+   +---------+    +---------+   +---------+
      | Ingress |---| Transit | ...| Transit |---| Egress  |
      |   Node  |   |   Node  |    |   Node  |   |   Node  |
      +---------+   +---------+    +---------+   +---------+
```

Figure 4 Hop-by-Hop Telemetry Type Mode

5.2. Telemetry Policy

Telemetry policy is used to determine which flow should be monitored. By configuring telemetry policy, it can increase the priority of learning and telemetry to critical flow and reduce or filter the learning and telemetry of unimportant flows. It is crucial to network deployment for two reasons, one is the number of flows can be huge, another is limited by telemetry processing capability either on the controller or the network node. There might be millions of flows in a large scale network, for example 5G mobile backhaul network. It is important to wisely choose the granularity of inband flow information telemetry. Regarding IP traffics, the telemetry policy can be based on either one of or combination of IP source/destination address, TCP/UDP port number, VRFs, or network device interfaces etc. To use an IP address with a flexible wildcard mask can be used as the telemetry to an aggregation of multiple flows. A flow identifier such as Flow-ID Label Indicator [I-D.ietf-mpls-inband-pm-encapsulation] or FlowMonID [I-D.ietf-6man-ipv6-alt-mark] is also used to identify a flow at transit or egress nodes.

5.3. Telemetry Deployment

In IFL, inband flow information telemetry is based on a class of flow characteristic and managed as an Inband Flow Information Telemetry Instance (IFITI). IFITI can be deployed on either controller or network node. When IFITI is created on controller and deployed from controller to network node. The network nodes including the ingress and egress node in E2E mode, as well as transit node in HbH mode are deployed with separate IFITI. It usually works in the need of an on-demand fault diagnose. When IFITI is created on network node, normally ingress node creates IFITI based on the received flow packets filtered and sampled by the pre-defined telemetry policy. Ingress node can also encode inband monitoring information in the flow packets. Transit or egress node detect the inband monitoring information of packets and automatically create IFITI to deploy the inband flow information telemetry. To create the IFITI on network node can greatly facilitate the dynamic and incremental deployment if needed.

The network node discovers the flow characteristic from the obtained service live traffic and sends it to the network controller. According to these flow characteristics, the network controller generates a Telemetry instance for monitoring the service flow. The network node obtains the instance and the corresponding identifier, such as Flow-ID, carries the identifier in the service flow to setup a relationship between the characteristic information, instance and the service flow, and performs Telemetry. The network controller also sends policies for the service discovery. The characteristic information extracting can base on the policy, preset cycle etc.

If the service message related to certain characteristic information is not received within the preset time, it is determined that the characteristic information is in an invalid state. And send the failure status information to the controller.

6. Inband Flow Information Telemetry Adjustment

When route convergence happens to the network, service flow may switch to other forwarding nodes. To monitor the same flow information, new telemetry instance is required to add on the new transit or egress node. Regarding the IFITI running on the fault path, the aging of IFITI should be supported in order to recycle the network resources. IFITI should be deleted once it becomes stale. Similar to the deployment of IFITI, aging and adjustment of IFITI can be controlled by the central controller or network node. When a specific timer used for flow information telemetry timeout, the IFITI would be deleted to stop the telemetry of the flow.

7. IANA Considerations

This document has no request to IANA

8. Security Considerations

TBD

9. References

9.1. 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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. Informative References

[I-D.hwyh-ippm-ps-inband-flow-learning] Han, L., Wang, M., Yang, F., and J. Huang, "Problem Statement and Requirement for Inband Flow Learning", Work in Progress, Internet-Draft, draft-hwyh-ippm-ps-inband-flow-learning-01, 25 October 2021, <https://www.ietf.org/archive/id/draft-hwyh-ippm-ps-inband-flow-learning-01.txt>.

[I-D.ietf-6man-ipv6-alt-mark] Fioccola, G., Zhou, T., Cociglio, M., Qin, F., and R. Pang, "IPv6 Application of the Alternate Marking Method", Work in Progress, Internet-Draft, draft-ietf-6man-ipv6-alt-mark-12, 22 October 2021, <https://www.ietf.org/archive/id/draft-ietf-6man-ipv6-alt-mark-12.txt>.

[I-D.ietf-mpls-inband-pm-encapsulation] Cheng, W., Min, X., Zhou, T., Dong, X., and Y. Peleg, "Encapsulation For MPLS Performance Measurement with Alternate Marking Method", Work in Progress, Internet-Draft, draft-ietf-mpls-inband-pm-encapsulation-02, 25 October 2021, <https://

www.ietf.org/archive/id/draft-ietf-mpls-inband-pm-encapsulation-02.txt>.

[I-D.ietf-opsawg-ntf] Song, H., Qin, F., Martinez-Julia, P., Ciavaglia, L., and A. Wang, "Network Telemetry Framework", Work in Progress, Internet-Draft, draft-ietf-opsawg-ntf-13, 3 December 2021, <https://www.ietf.org/archive/id/draft-ietf-opsawg-ntf-13.txt>.

[I-D.song-opsawg-ifit-framework] Song, H., Qin, F., Chen, H., Jin, J., and J. Shin, "A Framework for In-situ Flow Information Telemetry", Work in Progress, Internet-Draft, draft-song-opsawg-ifit-framework-17, 22 February 2022, <https://www.ietf.org/archive/id/draft-song-opsawg-ifit-framework-17.txt>.

Authors' Addresses

Liuyan Han
China Mobile
Beijing
China

Email: hanliuyan@chinamobile.com

Minxue Wang
China Mobile
Beijing
China

Email: wangminxue@chinamobile.com

Fan Yang
Huawei Technologies
Beijing
China

Email: shirley.yangfan@huawei.com