Problem Statement and Requirement for Inband Flow Learning
draft-hwyh-ippm-ps-inband-flow-learning-03

Abstract

   On-path telemetry techniques can provide high-precision inband flow
   insight and real-time network performance monitoring. Although they
   are benefical, network operators still face challenges applying such
   techniques, especially flow identification when deploying flow-
   oriented monitoring on a large scale. This document introduces the
   real network scenarios, and intends to address the problems by
   proposing the requirements of inband flow learning mechanism that can
   be used to implement inband flow information telemetry for
   deployability and flexibility.

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

   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 28 January 2024.

Copyright Notice

Table of Contents

1. Introduction

   On-path telemetry techniques can provide high-precision inband flow
   insight and real-time network performance monitoring (e.g., jitter,
   latency, packet loss) by embedding instructions or metadata into user
   packets. IOAM [RFC9197] and Alternate-Marking [RFC9341] are such
   techniques, and [RFC9197] [RFC9326] [RFC9343]
   [I-D.ietf-mpls-inband-pm-encapsulation] provide the encapsulations
   for different applications. By applying these techniques per-flow
   SLA compliance monitoring becomes available and benefical for network

operators, but there are still challenges as described in
[I-D.song-opsawg-ifit-framework]. Especially when deploying flow-
oriented monitoring on a large scale, the traditional static
configuration mode is no longer applicable.

Per-flow monitoring can be applied using network management tools,
such as Netconf YANG, to deliver the characteristics of specified
flows. Then network nodes can identify, match and monitor the flows
based on the characteristics. However, even though Netconf YANG can
provide feasibility to network operators, some problems or
inconveniences may occur during the deployment. For example, the
characteristic of a flow (e.g. IP 5-tupe) can vary dynamically and
mislead the service flow identification, or the monitored flow needs
to be reconfigured for the changes of the path. So inband flow
identification becomes a challenge in large scale deployment to
network operators. This document introduces the real network
scenarios, and intends to address the problems by proposing the
requirements of inband flow learning mechanism that can be used to
implement inband flow information telemetry for deployability and
flexibility. A proposed framework for inband flow learning mechanism
is described in [I-D.hwy-opsawg-ifl-framework], which is out of scope
of this document.

2. Terminology

   OAM: Operations, Administration, and Maintenance

   SLA: Service Level Agreement

   NFV: Network Function Virtualization

   UNI: User-Network-Interface

   CN: Core Network

3. Problem Statement

   The following sections describe scenarios that may occur in real
   network that make it difficult to deploy flow-oriented monitoring
   quickly and effectively at a large scale.

3.1. Frequent and Dynamic Change of Flows

   In 4G/5G mobile backhaul networks, IP address of one service can be
   changed based on location, time or even with business growth. The
   following scenarios describes the challenges which 4G/5G mobile
   service encounters.

3.1.1. Tidal Effect

A Tidal Effect phenomenon has been recognized as traffics between
base station and Core Network (CN) show repetitive patterns with
spatio-temporal variations. A typical example of Tidal phenomenon is
the traffic difference happened in day and night time of a commercial
and business area. In day time, eNodeB allocates more core network
resources when a large number of user equipment accesses eNodeB, and
less resources at night accordingly. The change of the number of UEs
and the core network resources may affect the change on source and
destination IP address of service flows.

Moreover, NFV used in core network makes the traffic change even
worse as the IP address at CN cannot be manually configured or even
predicted. In this case, it is impossible for operators to
statically deploy flow monitoring and statistics telemetry.

3.1.2. UPF Expansion

In 5G deployment, the increase of number of subscribers triggers the
expansion of UPF resources on data plane of 5G core network. After
new UPF resource is added, eNodeB sets up a connection to the new
UPF. Correspondingly, a new IP flow is created in mobile bearer
network. In this scenario, if flow monitoring and statistics
telemetry is deployed in a static mode, operators would need to
manually add related configurations to mobile bearer network after
the core network capacity is expanded, which is very difficult to
deploy in practice.

3.2. Enterprise Service Demand

The enterprise services usually connect different private networks
between Headquarter and Branches, Branches and Branches. Network
operator has very limited or even no information about end users.
Besides, information from one site could be changed from time to
time. Unpredictable information on enterprise customer side makes
impossible for network operators to set up real time flow monitoring,
and to avoid the omission of flow monitoring.

3.3. Large Scale Network Monitor Deployment and Maintenance

In a large-scale mobile bearer network, a large number of base
stations and corresponding access points may lead to a large number
of IP addresses in core network. From network maintenance
perspective, when flow monitoring and statistics telemetry is
deployed in a static mode, network operator had to manually set up
each monitoring instance between base station and core network, then
separately delegate configurations to a large number of network

entities. It is difficult for network operators to find an effective
way of monitoring creation and maintenance.

Note that traffic monitoring is comprised of uplink and downlink
directions, which makes twice of workload on configurations.

3.4. Service Flow Path Change

When a hop-by-hop flow monitoring is required by critical traffic for
deep SLA investigation, the actual forwarding path of service flow
and the every forwarding nodes along the path are obtained. Network
operator delegates different configurations to each node including
ingress, transit, and egress nodes on the path.

Once the traffic forwarding path is changed because of service flow
switching or route convergence, the monitoring instance on each node
needs to be re-deployed on the new path. In this situation, a
flexible and efficient deployment approach is required by network
operators.

4. Requirement

To face the flow deployment challenges mentioned in preceding
section, an approach of inband flow learning is required. It should
simplify the deployment of flow monitoring and achieve an automatic
mode of telemetry in large scale networks.

4.1. Ingress Flow Learning

On the UNI side of network node, ingress flow learning can help to
capture the characteristic data fields of packet and create the
monitoring instance when the flow is created from base station.
Flexible policy based on access control list (ACL) can facilitate the
identification of flow characteristic. For example, IP 2-tuple
(DIP+SIP), DSCP value, etc.

4.2. Egress Flow Learning

Similar to the requirement on ingress node, traffic egress node
should support the same capability of inband flow learning to create
traffic monitoring instance for completing a monitor. When the
egress node or egress port of a service flow is changed, the egress
node or egress port of service flow can be triggered to re-learn and
re-monitor the service flow.

4.3. Hop-by-Hop Flow Learning

When hop-by-hop flow monitoring and telemetry is required, the flow learning and monitor deployment should be created on all the ingress, transit, and egress nodes that service flows pass through. When the path of a service flow changes due to the service switching or network convergence, the service flow re-triggers the flow learning on the new path and starts the new monitoring of service flow.

4.4. Auto Flow Aging

In all the inband flow learning scenarios described above, when the path of a service flow changes, the flow learning on new path is triggered and new monitoring instances are created on devices. Regarding the monitoring instances that have been created before the path change, if there is no traffic detected within a certain period of time, automatic aging and resource recycle should be supported.

4.5. Flow Learning Policy

It is valuable to specify the flow learning policy on equipment when thousands or millions of flows are transmitted. Flow learning policy specifies the metrics and explicit rules executed on equipment, for example the flow is filtered based on a particular range of protocol number. Centralized controller specifies the flow learning policy via management and control plane to equipment, then data plane executes the policies to generate monitoring instance.

5. IANA Considerations

This document has no request to IANA

6. Security Considerations

TBD

7. References

7.1. 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>.

7.2. Informative References

   [I-D.hwy-opsawg-ifl-framework]
              Han, L., Wang, M., Wang, X., and T. Zhou, "Inband Flow
              Learning Framework", Work in Progress, Internet-Draft,
              draft-hwy-opsawg-ifl-framework-03, 3 July 2023,
              <https://datatracker.ietf.org/doc/html/draft-hwy-opsawg-
              ifl-framework-03>.

   [I-D.ietf-mpls-inband-pm-encapsulation]
              Cheng, W., Min, X., Zhou, T., Dai, J., and Y. Peleg,
              "Encapsulation For MPLS Performance Measurement with
              Alternate Marking Method", Work in Progress, Internet-
              Draft, draft-ietf-mpls-inband-pm-encapsulation-06, 14 June
              2023, <https://datatracker.ietf.org/doc/html/draft-ietf-
              mpls-inband-pm-encapsulation-06>.

   [I-D.song-opsawg-ifit-framework]
              Song, H., Qin, F., Chen, H., Jin, J., and J. Shin,
              "Framework for In-situ Flow Information Telemetry", Work
              in Progress, Internet-Draft, draft-song-opsawg-ifit-
              framework-20, 24 April 2023,
              <https://datatracker.ietf.org/doc/html/draft-song-opsawg-
              ifit-framework-20>.

   [RFC9197] Brockners, F., Ed., Bhandari, S., Ed., and T. Mizrahi,
              Ed., "Data Fields for In Situ Operations, Administration,
              and Maintenance (IOAM)", RFC 9197, DOI 10.17487/RFC9197,
              May 2022, <https://www.rfc-editor.org/info/rfc9197>.

   [RFC9326] Song, H., Gafni, B., Brockners, F., Bhandari, S., and T.
              Mizrahi, "In Situ Operations, Administration, and
              Maintenance (IOAM) Direct Exporting", RFC 9326,
              DOI 10.17487/RFC9326, November 2022,
              <https://www.rfc-editor.org/info/rfc9326>.

   [RFC9341] Fioccola, G., Ed., Cociglio, M., Mirsky, G., Mizrahi, T.,
              and T. Zhou, "Alternate-Marking Method", RFC 9341,
              DOI 10.17487/RFC9341, December 2022,
              <https://www.rfc-editor.org/info/rfc9341>.

   [RFC9343] Fioccola, G., Zhou, T., Cociglio, M., Qin, F., and R.
              Pang, "IPv6 Application of the Alternate-Marking Method",
              RFC 9343, DOI 10.17487/RFC9343, December 2022,
              <https://www.rfc-editor.org/info/rfc9343>.

Authors' Addresses

   Liuyan Han
   China Mobile
   Beijing
   China
   Email: hanliuyan@chinamobile.com

   Minxue Wang
   China Mobile
   Beijing
   China
   Email: wangminxue@chinamobile.com

   Xuanxuan Wang
   Huawei Technologies
   Beijing
   China
   Email: wxxuan@huawei.com

   Jinming Huang
   Huawei Technologies
   Dongguan
   China
   Email: zhangshengli4@huawei.com