

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: 6 September 2022

X. He  
X. Mao  
China Telecom  
Q. Ma  
X. Zhou  
Huawei  
5 March 2022

Problem Statement and Use Cases of Adaptive Traffic Data Collection  
draft-he-adaptive-collecting-problem-usecases-00

## Abstract

IP carrier network needs to provide real-time traffic visibility to help network operators quickly and accurately locate network congestion and packet loss, and make timely path adjustment for deterministic services in order to avoid congestion. It is essential to explore the adaptive traffic data collection mechanism so as to capture real-time network state at minimum resource consumption.

This document summarizes the problems currently faced by network operators when attempting to provide timely traffic data collection to satisfy the various scenarios that require real-time network state and traffic visibility, and aggregates the requirements for adaptive traffic collecting mechanism from a variety of deployment scenarios.

## 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 6 September 2022.

## 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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">1.1.</a>	Abbreviations . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Problem Statement . . . . .	<a href="#">4</a>
<a href="#">4.</a>	Scenarios of Adaptive Traffic data collection . . . . .	<a href="#">6</a>
<a href="#">4.1.</a>	Multi-dimensional real-time portrait of interface traffic characteristic . . . . .	<a href="#">6</a>
<a href="#">4.2.</a>	Microburst traffic detecting . . . . .	<a href="#">6</a>
<a href="#">4.3.</a>	Congestion avoidance for deterministic services . . . . .	<a href="#">7</a>
<a href="#">4.4.</a>	On-path telemetry based on adaptive traffic sampling . . . . .	<a href="#">7</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">8</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">8</a>
<a href="#">7.</a>	References . . . . .	<a href="#">8</a>
<a href="#">7.1.</a>	Normative References . . . . .	<a href="#">8</a>
<a href="#">7.2.</a>	Informative References . . . . .	<a href="#">9</a>
	Authors' Addresses . . . . .	<a href="#">9</a>

## [1.](#) Introduction

With the advent of cloud computing, big data and AI, as well as the scale deployment of 5G mobile communication technology, a large number of uRLLC services such as AR/VR, industrial Internet and computing power network have emerged, which puts forward higher requirements for the service quality of IP carrier network. IP carrier network needs to provide real-time traffic visibility to help network operators quickly and accurately locate network congestion and packet loss, and make timely path adjustment for the services of deterministic delay in order to avoid the congested nodes and links. For such business scenarios, the network needs to provide traffic sampling capability in sub seconds or even milliseconds so as to gain real-time network state.

For decades, SNMP and MIBs have been widely deployed and the de facto choice for many monitoring solutions, especially in collecting interface traffic. Arguably the biggest shortcoming of SNMP for those applications concerns the need to rely on periodic polling, because it introduces an additional load on the network and devices,

and it is brittle if polling cycles are missed. Therefore, SNMP has no capability to realize real-time traffic sampling at sub seconds or even milliseconds level. Telemetry, as a revolutionary data acquisition technique, based on pull mechanism that is able to deliver object changes as they happen, overcomes the limitations of SNMP such as "slow speed, low efficiency and more demands for processing capacity". Nevertheless, for the sake of capturing real-time network state, persistent sampling of interface traffic at milliseconds interval will generate a considerable amount of data which may claim too much transport bandwidth and overload the servers for data collection, storage, and analysis. Increasing the data handling capacity is technically feasible but expensive, and difficult to achieve large-scale deployment in operator's networks. It is essential to explore the adaptive traffic data collection mechanism so as to capture real-time network state at minimum resource consumption.

This document summarizes the problems currently faced by network operators when attempting to provide timely traffic data collection to satisfy the various requirements by the aforementioned new scenarios that require real-time network state and traffic visibility. Also, this document aggregates the requirements for adaptive traffic data collection mechanism from a variety of deployment scenarios.

### [1.1](#). Abbreviations

AI: Artificial Intelligence

AR: Augmented Reality

VR: Virtual Reality

IP RAN: IP Radio Access Network

DetNet: Deterministic Networking

QoE: Quality of Experience

SLA: Service Level Agreement

He, et al.

Expires 6 September 2022

[Page 3]

---

Internet-Draft

Adaptive Traffic Data Collection

March 2022

uRLLC: ultra Reliable & Low Latency Communication

NMS: Network Management System

IDC: Internet Data Center

SNMP: Simple Network Management Protocol

MIB: Management Information Base

## [2.](#) Terminology

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.

The following terms are defined in this document:

adaptive traffic data collection: Allow servers automatically switch to different telemetry sampling period to collect traffic data according to the threshold change.

### 3. Problem Statement

As is well known, IP network, based on statistical multiplexing model, is of traffic burst characteristics. For a long time, operators have obtained traffic visibility from the Network Management System (NMS), and satisfied with 30~40% bandwidth utilization. In spite of such low link usage, many complaints have still been received about poor QoE in delivering applications with the sensitivity of delay and packet loss. The fundamental cause is that the observed average network traffic masks the characteristics of traffic burst, given that SNMP is widely employed in operator's networks to collect network traffic at 5 minutes intervals.

A large quantity of laboratory data and operational data indicate that a microburst phenomenon occurs frequently in operator's carrier networks, such as IP RAN, IP metropolitan network, IP backbone network and IDC. The typical duration of such a microburst is tens to hundreds of milliseconds, easy to cause instantaneous congestion

of the output queue. Network congestion amplifies queuing delay and jitter, it may even give rise to packet loss. All along, solving the problem of network congestion is a major challenge for IP networks. So, the microburst is not beneficial to the deterministic-delay applications. And it is difficult to eliminate the microburst, but must attempt to avoid it.

Although the mechanism of microburst is not very distinct, however, it does not hinder us to detect it. Fortunately, Telemetry (e.g., YANG PUSH [[RFC8639](#)] [[RFC8641](#)], gNMI [[gNMI](#)]) has the capability to collect interface traffic at a higher frequency, i.e., millisecond interval. So, by means of telemetry technique, we can capture the complete aspects of a microburst traffic. However, it is impractical to gain the real-time traffic visibility at the cost of persistent sampling at millisecond intervals. For example, in order to capture a microburst traffic of interface, at least 10-millisecond sampling cycle is necessary. Compared with the today's widely employed 5-minute sampling cycle based on SNMP, the required resources will increase by 30000 times!

It is essential to investigate the adaptive traffic data collection mechanism so as to capture real-time network state at minimum

resource consumption. That is to say, in normal non-congested network conditions, which happen at the time of 95% above, minutes-level sampling cycle is enough as it is. But, while detecting a congestion state or congestion trend, sampling period must be timely tuned to milliseconds to capture a microburst traffic of interface. A congestion state or congestion trend of interface is manifested by packet loss due to queue overflow, queue depth beyond the threshold or too high link utilization, which can be defined as Event-triggered data. Such data can be actively pushed through subscription or passively polled through query. Although the microburst phenomenon occurs frequently, it is transient and an on-line detection tool is preferable to find it timely. The traditional method of using CPU on main control board through query is processing resources consuming, the network device must possess built-in hardware designed especially to monitor it.

In order to reduce the excessive consumption of resources caused by millisecond level collection of the single data, batch data such as hundreds of sampled traffic data from an interface can be packaged as a telemetry packet and is sent to the collector. The timestamp is required for every sampled traffic data for the convenience of the collector visualizing the interface traffic trend, And the collector must realize traffic visualization in real-time manner in order that the operators can observe it immediately.

#### [4.](#) Scenarios of Adaptive Traffic data collection

This section presents several typical scenarios which require adaptive traffic data collection to gain real-time network state and traffic visibility at minimum resource consumption.

##### [4.1.](#) Multi-dimensional real-time portrait of interface traffic characteristic

Interface traffic data collection is one of the most important functions for NMS. Today, more and more applications are of latency-sensitive and loss-sensitive characteristic, and the real-time traffic visibility can help operators better understand network performance so as to achieve SLA guarantees. On the other hand, obtaining the holistic and genuine characteristic of interface

traffic is also a basic requirement for the statistical multiplexing model of IP network, which is of great significance for traffic prediction, network planning, network capacity expansion, network optimization, etc. However, the traditional NMS based on SNMP has no capability to depict genuine characteristic of interface traffic, and interface traffic data collection based on telemetry techniques is preferable.

It is essential to exploit the adaptive traffic data collection techniques to depict multi-dimensional real-time portrait of interface traffic characteristic at minimum resource consumption. That is to say, in normal non-congested network conditions, which happen at the time of 95% above, minutes-level sampling cycle is enough as it is. But, while detecting a congestion state or congestion trend, sampling cycle must be timely tuned to milliseconds to capture a microburst traffic of interface. Such an adaptive traffic data collection technique can not only reflect the coarse-grained interface traffic characteristics, but also capture the congestion state of interface with finer time granularity. It will be an important tool for the DetNet to obtain real-time network performance. Because of the lower cost, it can be deployed on large-scale in operator's networks.

#### [4.2.](#) Microburst traffic detecting

Microburst traffic, as an instantaneous congestion phenomenon occurring frequently in IP carrier network, will cause critical delay jitter and even packet loss, which will seriously affect the QoE of latency-sensitive and loss-sensitive applications. The ability of detecting microburst traffic of interface will help network operators quickly and accurately locate network congestion and packet loss, and make timely path adjustment for deterministic-delay services in order to avoid the congested nodes and links.

Because the typical duration of such a microburst is generally tens to hundreds of milliseconds, at least 10-millisecond sampling cycle is necessary. Although the microburst phenomenon occurs frequently, it takes very little time of 24 hours a day. It is not a good approach to observe it through persistent millisecond sampling period. Preferably, we can capture it as soon as a microburst occurs to ensure important diagnose data will not be missed. Because it is transient and an on-line detection tool is required to find it

timely. Triggered by the events such as packet loss, queue depth beyond the threshold which is detected timely, sampling period must be timely tuned to milliseconds to capture a microburst traffic of interface. In a word, it is of practical significance to explore the microburst detection technology aiming at minimizing resource consumption.

#### [4.3.](#) Congestion avoidance for deterministic services

Network congestion will rapidly increase queuing delay and jitter, it may even give rise to packet loss, which will seriously affect the QoE of delay-sensitive and packet loss-sensitive applications. The goal of network optimization is to reduce the occurrence of network congestion as much as possible.

It is a complicated problem for network operators to accurately predict the trend of network congestion and make network adjustment in advance. The real-time traffic visibility based on the adaptive traffic data collection techniques can accurately predict the long-term congestion, and quickly capture the instantaneous congestion (i.e., microburst) of interface. By means of the real-time traffic visibility, the automatic optimization tool (e.g., AI) can make timely path adjustment for key traffic flows. For example, based on the real-time traffic visibility and microburst events (e.g., packet loss, queue depth) collected, the controller can accurately predict the congestion trend of interface and make timely traffic redirection to the non-congested interface for delay deterministic applications.

#### [4.4.](#) On-path telemetry based on adaptive traffic sampling

On-path telemetry is useful for application-aware networking operations. For example, it is critical for the operators who offer high-bandwidth, latency and loss-sensitive services such as video streaming and online gaming to closely monitor the relevant flows in real-time as the basis for any further optimizations. Applying on-path telemetry on all packets of selected flows can still be out of reach. A sampling rate should be set for these flows and only enable telemetry on the sampled packets. However, a too high rate would exhaust the network resource and even cause packet drops; an overly low rate, on the contrary, would result in the loss of information

An adaptive approach can be used based on the network conditions to dynamically adjust the sampling rate. In normal network state, a low sampling rate is enough to reflect network performance; But, in case of network congestion, the controller is aware of it from the real-time traffic visibility and events data collected (e.g., packet loss, queue depth), and timely adjust the packet sampling rate at very high level. Even all packets of selected flows are applicable so as to acquire real-time measurement data such as latency, jitter and packet loss.

## 5. IANA Considerations

This document does not include an IANA request.

## 6. Security Considerations

This document provides an adaptive telemetry mechanism to minimize the resource consumption. The increased complexity of network telemetry may give rise to some security concerns. For example, persistent traffic collection at very high rate (e.g., at millisecond interval) induced by wrong configuration or spurious triggering might exhaust resources of the forwarding plane and the control plane of network device as well as the collector; An inappropriate threshold setting should be avoided. The telemetry data is highly sensitive, which exposes a lot of information about the network and its configuration. Some of that information can make designing attacks against the network much easier (e.g., exact details of what software and patches have been installed), and allows an attacker to determine whether a device may be subject to unprotected security vulnerabilities.

On the other hand, for telemetry interfaces security considerations, NETCONF or gNMI must provide authentication, data integrity, confidentiality, and replay protection. And further study of the security issues will be required.

## 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>>.

- [RFC3688] Mealling, M., "The IETF XML Registry", [BCP 81](#), [RFC 3688](#), DOI 10.17487/RFC3688, January 2004, <<https://www.rfc-editor.org/info/rfc3688>>.
- [RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", [RFC 6020](#), DOI 10.17487/RFC6020, October 2010, <<https://www.rfc-editor.org/info/rfc6020>>.
- [RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", [RFC 6242](#), DOI 10.17487/RFC6242, June 2011, <<https://www.rfc-editor.org/info/rfc6242>>.
- [RFC8639] Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E., and A. Tripathy, "Subscription to YANG Notifications", [RFC 8639](#), DOI 10.17487/RFC8639, September 2019, <<https://www.rfc-editor.org/info/rfc8639>>.
- [RFC8641] Clemm, A. and E. Voit, "Subscription to YANG Notifications for Datastore Updates", [RFC 8641](#), DOI 10.17487/RFC8641, September 2019, <<https://www.rfc-editor.org/info/rfc8641>>.

## [7.2](#). Informative References

- [gNMI] "https://github.com/openconfig/gnmi".
- [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>>.

## Authors' Addresses

Xiaoming He  
China Telecom  
Email: hexm4@chinatelecom.cn

Dongfeng Mao  
China Telecom  
Email: maodf@chinatelecom.cn

Qiufang Ma  
Huawei  
101 Software Avenue, Yuhua District  
Nanjing

Jiangsu, 210012  
China

He, et al.

Expires 6 September 2022

[Page 9]

---

Internet-Draft

Adaptive Traffic Data Collection

March 2022

Email: [maqiufang1@huawei.com](mailto:maqiufang1@huawei.com)

Tianran Zhou

Huawei

Email: [zhoutianran@huawei.com](mailto:zhoutianran@huawei.com)

