INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG11-TD209/GEN

STUDY GROUP 11

Original: English

Question(s): 13/11 Geneva, 6-15 July 2022

TD

Source: Editors

Title: Output - baseline text of new work item TR.MPLRA "Technical report on requirements and architecture for monitoring packet loss caused by network congestion" (Geneva, 6-15 July 2022)

Contact: Xiaoming He
China Telecom
P.R.China
Tel: + 86 13316097161
E-mail: hexm4@chinatelecom.cn

Contact: Minrui Shi
China Telecom
P.R.China
Tel: + 86 18918588657
E-mail: shimr@chinatelecom.cn

Contact: Yongsheng Liu
China Unicom
P.R.China
Tel: + 8610 68799999
E-mail: liuys170@chinaunicom.cn

Contact: Jinyou Dai
CICT (China Information Communication Technologies Group)
P.R.China
Tel: +86-02787693442
E-mail: djy@cict.com

Abstract: This document is the baseline text of draft new technical report TR.MPLRA "Technical report on requirements and architecture for monitoring packet loss caused by network congestion" which is initiated at Q13/11 meeting held on 6-15 July 2022 in Geneva.

The following table shows discussion results for input documents.

Document Number	Source	Title	Meeting results
SG11-C0049	China Telecom	Proposal for initiating a new work item on requirements and architecture for monitoring packet loss caused by network congestion	Due to the time limitation, clause 7 is put into square brackets for further review.

Draft new Technical Report ITU-T TR.MPLRA

Technical report on requirements and architecture for monitoring packet loss caused by network congestion

Summary

This technical report studies the requirements and architecture for monitoring packet loss caused by network congestion, including:

- General requirements for monitoring packet loss caused by network congestion
- Architecture for monitoring packet loss caused by network congestion
- Interfaces requirements for monitoring packet loss caused by network congestion
- Security of considerations

Keywords

Monitoring packet loss; network congestion; requirements; architecture

Table of Contents

Draft new Technical Report ITU-T TR.MPLRA

Technical report on requirements and architecture for monitoring packet loss caused by network congestion

1. Scope

This technical report studies the requirements and architecture for monitoring packet loss caused by network congestion.

The scope of this technical report includes:

- General requirements for monitoring packet loss caused by network congestion
- Architecture for monitoring packet loss caused by network congestion
- Interfaces requirements for monitoring packet loss caused by network congestion
- Security of considerations

2. References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this technical report. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this technical report are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this technical report does not give it, as a stand-alone document, the status of a Recommendation.

TBD

3. Definitions

3.1. Terms defined elsewhere

This technical report uses the following terms defined elsewhere:

TBD

3.2. Terms defined in this technical report

This technical report defines the following terms:

3.2.1 Network telemetry: The process for acquiring and utilizing network data remotely for network monitoring and operation, concerning aspects like data generation, collection, correlation, and consumption.

4. Abbreviations and acronyms

This technical report uses the following abbreviations and acronyms:

AM	Alternate Marking
DetNet	The Deterministic Networking
eMBB	Enhanced Mobile Broadband

IP Internet Protocol

iOAM in-situ Operation, Administration and Maintenance

MAC Media Access Control

MPLS Multi-Protocol Label Switching

OAM Operation, Administration and Maintenance

SR Segment Routing

RPC Remote Procedure Call

TWAMP Two-Way Active Measurement Protocol

TCP Transmission Control Protocol

uRLLC ultra-low Delay and High Reliability Communication

VPN Virtual Private Network

5. Conventions

In this technical report:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this technical report is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this technical report.

6. Overview

Contributor's note: this section presents the overview of monitoring packet loss caused by network congestion.

In the 5G era, the emerging services such as enhanced mobile broadband (eMBB) and ultra-low delay and high reliability communication (uRLLC) have put forward higher requirements for the service quality of bearer networks (i.e., more less delay, more less jitter and more less packet loss). The "best of effort" service mode of traditional IP network is unsustainable, and the deterministic network (DetNet) comes into being. On the other hand, the statistical multiplexing model of IP network based on TCP/IP protocol determines that the network traffic is of burst characteristic. Congestion is a common phenomenon in IP network. Network congestion leads to the deterioration of network performance and increases the uncertainty of service delivery. In order to reduce the uncertain services caused by network congestion, it is necessary to monitor the status and trend of network congestion in real-time manner, evaluate the level of network congestion, and provide basis for network planning, capacity expansion and optimization. The existing monitoring and measurement methods, including active measurement methods (e.g., Y.1564, Y.1731, IP Ping, TWAMP [RFC5357], RFC2544, etc.) and hybrid measurement methods (e.g., in-situ OAM [i-d.ietf-ippm-ioam-data], alternate marking (AM) [RFC8321], etc.), cannot reflect the genuine congestion level of the network, especially lack of effective means to accurately pinpoint the congestion location and accurately detect the number of discarded packets caused by congestion.

In view of this, the research on real-time congestion and packet loss monitoring technique is of great significance. This draft technical report does not attempt to replace the existing packet loss measurement techniques, but to make up for the shortcomings of the existing techniques. As an auxiliary tool of the existing measurement techniques, it helps the network operators or by the automatic operation and maintenance tools to quickly pinpoint the congested nodes and affected traffic flows, and improve the efficiency of fault diagnosis and root cause analysis.

7. [General requirements for monitoring packet loss caused by network congestion]

Contributor's note: the requirements for monitoring packet loss caused by network congestion will be presented in this section.

7.1. [Requirements of network elements for monitoring packet loss caused by congestion

The requirements of network elements for monitoring packet loss caused by network congestion include:

- Network element is required to support Dynamic subscriptions, where a subscriber initiates a subscription negotiation with a publisher via an RPC.
- Network element is required to support Configured subscriptions, which allow the management of subscriptions via a configuration.
- Network element is required to support the ability to subscribe to periodic updates. The subscription period shall be configurable as part of the subscription request.
- For periodic subscription, network element is recommended to support the ability of the redundant suppress, where a telemetry update should not be generated unless the value of the subscribed data objects has changed.
- Network element is required to support the ability to subscribe to updates on-change, i.e., whenever values of the subscribed data objects change.
- For on-change subscription, network element is required to support a dampening period that needs to be passed before the first or subsequent on-change updates are sent. The dampening period should be configurable as part of the subscription request.
- Network element is required to detect packet loss caused by congestion timely (i.e., millisecond interval) by the dedicated hardware.
- Network element is required to report packet loss event in real-time manner, including the time of packet loss occurrence, the number of discarded packets, the localization of packet loss such as element ID, port ID, queue ID.
- Network element is required to report packet loss event periodically.
- Network element is required to report packet loss event on-change.
- Network element is required to cache all discarded packets.
- Network element is required to upload all discarded packets cached in real-time manner.
- Network element is required to support time synchronization for measuring packet loss ratio caused by congestion, and time synchronization accuracy is less than 50ms.
-

7.2. Requirements of collection and analysis system for monitoring packet loss caused by congestion

The requirements of collection and analysis system for monitoring packet loss caused by network congestion include:

- It is required to support Configured subscriptions as server, accepting subscription data.
- It is required to support Dynamic subscriptions as client, initiating subscription request and accepting subscription data.
- It is required to collect packet loss event for statistics and analysis.
- It is required to support data repository for storing all discarded packets uploaded.
- It is required to analyse the service types of discarded packets, and count the number of discarded packets of each traffic flow in real-time manner.
- It is required to support the ability of analysing IP packet header, including source or destination MAC address, source IP address or N-tuple, MPLS or SR label, VPN ID, VLAN ID, and so on, so as to determine traffic flow ID of every discarded packet.
- It is required to support measurement of packet loss ratio according to the number of the discarded packets divided by the number of the sent packets for the specified user service traffic.
- It is required to support traditional data analysis methods (e.g., statistical analytical method, visualization analytical method, correlation analytical method) to process the discarded packets.
- It is recommended to support advanced big-data and Machine learning techniques to process data of the discarded packets, such as forecasting congestion trend, fixing the cause of congestion, etc.
- It is required to support visualization of data analysis for the discarded packets in the form of tables and figures, which are easily understandable to users.
-]

8. Architecture for monitoring packet loss caused by network congestion

Contributor's note: the architecture for monitoring packet loss caused by network congestion will be described in this section.

The architecture for monitoring packet loss caused by congestion is mainly composed of network elements and collection and analysis system. All network elements of IP network need to report the packet loss events caused by congestion to the collection and analysis system in real-time manner, and also cache the discarded packets overflowed by the port queue and upload them to the collection and analysis system. The collection and analysis system counts the total number of discarded packets reported, analyses the service types of discarded packets, and counts the number of discarded packets of each traffic flow, and so on. This monitoring mode of "zero intervention" on the network can not only accurately locate packet loss caused by congestion, determine the time of packet loss occurence, and accurately count the number of the discarded packets and the type of traffic flow which they belong to, but also be used as an auxiliary means of packet loss measurement to achieve more accurate measurement results. Therefore, it is of significance for network congestion real-time monitoring. Figure 1 illustrates the proposed architecture for monitoring packet loss caused by congestion.

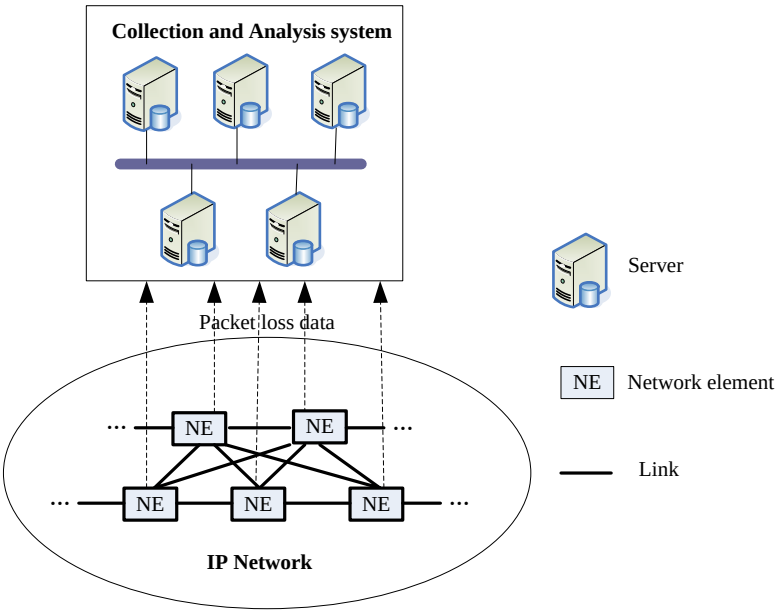

Figure 1 Architecture of monitoring packet loss caused by congestion

8.1. Network element

8.2. Collection and analysis system

9. Interfaces requirements

10. Security considerations