SFC Working Group
INTERNET-DRAFT
Intended Status: Standards Track
Expires: December 30, 2016

Anil Kumar S N
Gaurav Agrawal
Vinod Kumar S
Huawei Technologies India
June 28, 2016

Packet Loss Measurement for SFC
draft-agv-sfc-packet-loss-measurement-01

Abstract

This document describes performance measurement(PM) packet loss measurement for Service Function Chains (SFCs) to assess the operational status and behavior of a SF, a subset of SFs, a whole SFC as a function of the actual deterministic SF/SFC. Packet loss mechanism described in this document is based on [SFC-PM-arch]

Table of Contents

1 Introduction

The delivery of end-to-end services often requires various service functions. These include traditional network service functions such as firewalls and traditional IP Network Address Translators (NATs), as well as application-specific functions. The definition and instantiation of an ordered set of service functions and subsequent "steering" of traffic through them is termed Service Function Chaining (SFC).

The common reasons for packet drop are traffic congestion, service function (DPI/Firewall/Router etc.) performance issue, software issues (bugs), faulty hardware or cabling and service function processing errors.

Proper operation of a SFC depends on the ability to monitor and quickly identify faults and focus attention on the root cause of the problem. Also service provider service level agreements (SLAs) depends on the capability to measure and monitor performance metrics for packet delay. SFC delay measurement is one of the important tool to achieve above requirements.

Packet loss measurement capability provides operators with greater visibility into the performance characteristics of their networks, thereby facilitating planning, troubleshooting, and network performance evaluation.

This document specifies best possible efficient and accurate mechanism for packet loss measurement for service function chains (SFCs) for a SFC network domain.

The packet loss measurement described in this document is realized by adding a new context header in the network service header.

1.1 Terminology

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 Terms & Definition

Refer to RFC 7665 for definitions of SFC terms.

Measurement Collector: An operational function that collects measurement data from a measurement agent. Measurement collector is responsible for collecting the performance measurement data from measurement agent. Measurement collector functionality could be integrated with one of the MA or with the controller itself.

Measurement Agent: An operational function that contains one or more measurement functions. Measurement agents is responsible for understand and analyze performance measurement control information encoded in NSH metadata and perform the performance data collecting and report the same to measurement collector with key information to identify performance measurement instance along with data collected.

Measurement Controller: An operational function that controls running, scheduling, and general coordination of measurement functions by instructing a measurement agent using NSH metadata. Measurement controller is responsible for configuring the performance measurement instance. Optionally performance measurement instance can be configured manually at the ingress in which case controller is not required

1.3 Applicability and Scope

This document defines the implementation mechanism for the packet loss measurement as per performance measurement architecture [SFC-PM-arch]. This document defines a new NSH message format for carrying packet loss measurement related control information. It also defines operations to be carried out for packet loss measurement. communication mechanism between measurement controller, measurement collector and MA is out of scope of this document.

2 Massage Format

2.1 Performance Measurement Context Header

The format of the Performance measurement context headers, is as described below.

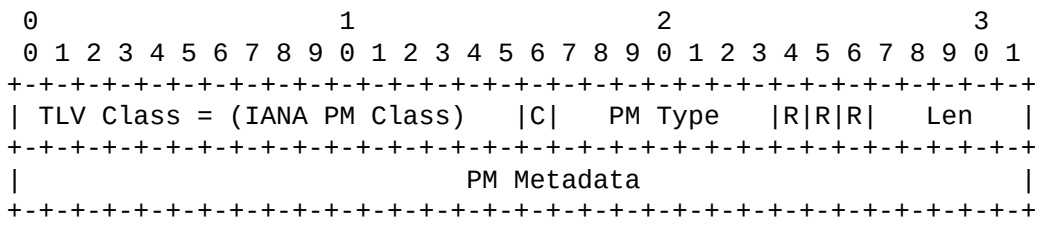


Figure 1: Performance Measurement Context Header

TLV Class: As per [I-D.ietf-sfc-nsh] the TLV class value for performance measurement needs to be applied from IANA.

PM Type: indicates the type of performance measurement that needs to be carried out by the MA.

Length: Length of the variable PM metadata, in 4-byte words.

2.2 Packet Loss PM Context Header

The format of the packet loss PM context headers, is as described below.

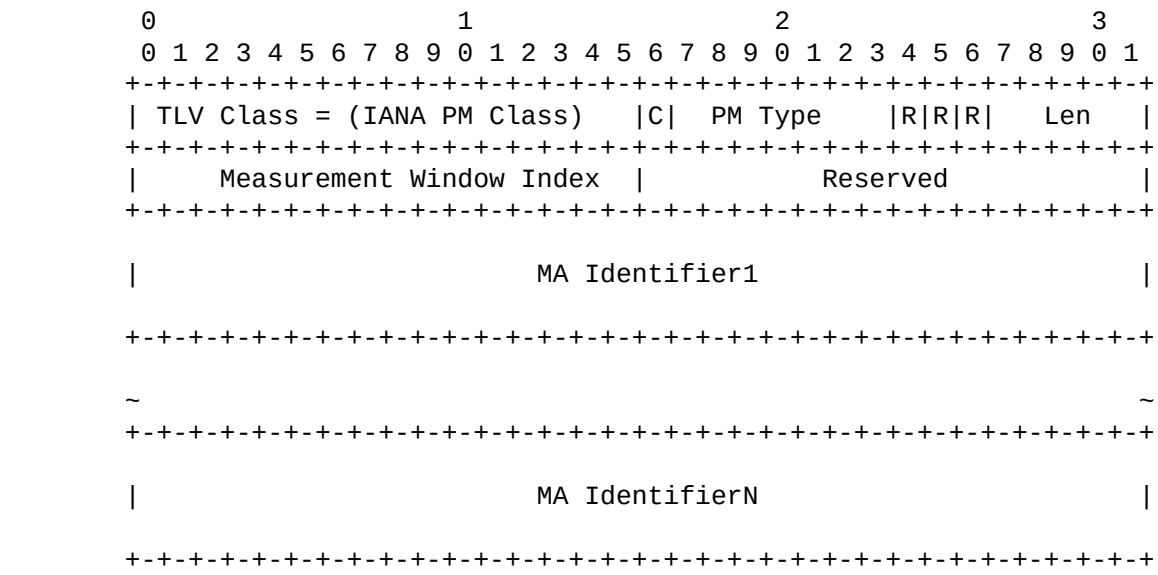


Figure 2: Packet Loss PM Context Header

TLV Class: As per [I-D.ietf-sfc-nsh] the TLV class value for performance measurement needs to be applied from IANA.

PM Type: Indicates the type of performance measurement that needs to be carried out by the MA. (IANA assigned PM Type PM Loss value)

This memo defines the following values.

0x1 - Packet Loss : indicates PM meta data contains info for packet loss. Specified SF(s) SHOULD participate in packet loss PM.

0x2 - SF Hop by Hop Packet Loss : indicates PM meta data contains info for packet loss. All the SF(s) in the SFP SHOULD participate in the packet loss PM

0x3 - SFF Hop by Hop Packet Loss : indicates PM meta data contains info for packet loss. All the SFF(s) in the SFP SHOULD participate in the packet loss PM

0x4 - All Hop by Hop Packet Loss : indicates PM meta data contains info for packet loss. All the SF(s) and SFF(s)in the SFP SHOULD participate in the packet loss PM

0x5 - SFP as a whole : indicates PM meta data contains information for packet delay. Classifier (source MA) and SF domain boundary SFF (sink MA) SHOULD participate in the packet delay computation.

Additional values can be added for future PM types and scenarios.

Length: Length of the variable PM metadata, in 4-byte words. It will have a minimum length of 1 indicating the presence of measurement window index.

Measurement Window Index: 16 bit number to denote the current measurement window to which the packet belongs.

Reserved: Reserved 16 bits for future purpose.

Reserved: Reserved 16 bits for future purpose.

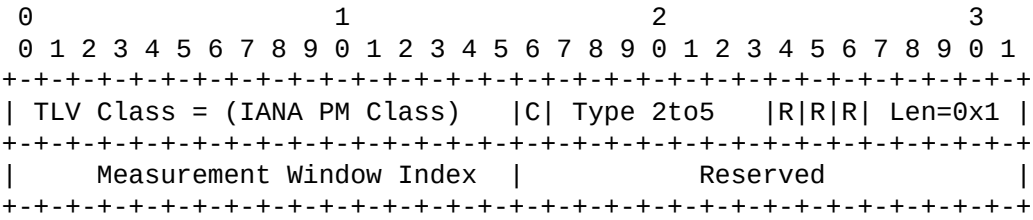
MA identifier list: List of participating MA in the SFP.

MA identifier has two parts

1) Node identifier - 24 bit
   a) For SFF: MUST be unique number assigned by controller
   b) For SF: All zero. Context identifier itself identifies SF node.
2) Context identifier - 8 bit
   a) For SFF: Service index of next SF.
   b) For SF: Service index

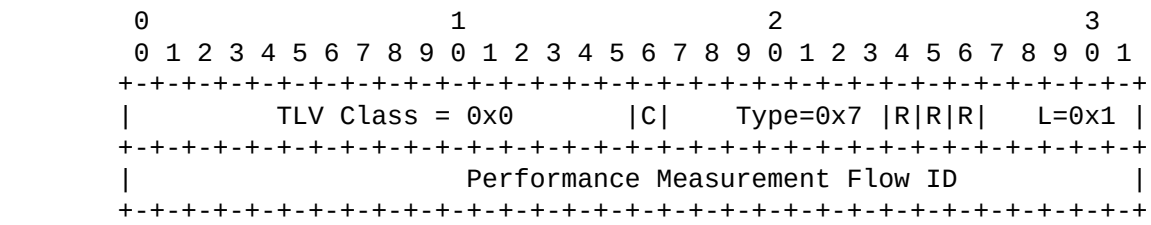
MA identifier SHOULD be in decreasing order of the SI for optimized traversal of the SI participation.

The Length of the packet loss PM context headers, is fixed to 1 as described below, when the PM Type is 2 to 5. Since all SF's in the SFP has to perform the loss measurement specified in PM type field.

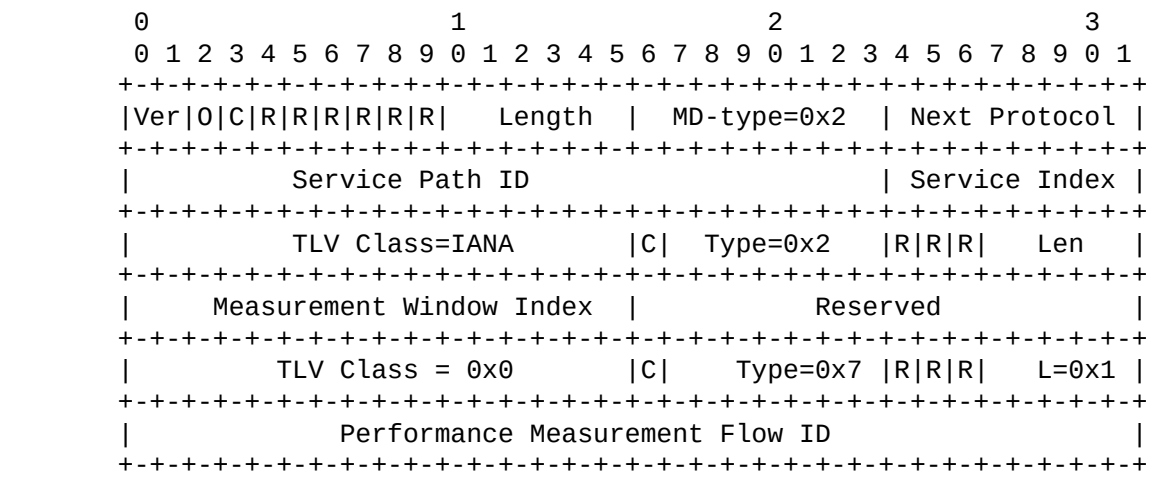


2.3 Performance Measurement Flow ID

The method of encoding the PMF id is done using the flow id defined in [I-D.ietf-sfc-nsh].



Sample encoding of PMF using flow ID



3 Operations

3.1 Packet Loss Statistics Counter

Every MA needs to maintain the packet loss statistics which they immediately report it to collector or may accumulate and report to collector at a reporting interval which depends on local policy.

Below 2 packet statistics counters will be created and maintained at every MA

1) Rx-STAT[P][M][W]

2) Tx-STAT[P][M][W]

Rx-STAT[P][M][W]: This 2 dimensional statistics counter is maintained at every MA. Where P stands for PMF ID, M stands for MA identifier and W stands for window ID. Rx- STAT[P][M][W] counter maintains the number of packets received for a given PMF ID + MA identifier + window. PMF ID is unique within a SFC Domain, for a given PMF ID there could be multiple windows. Rx-STAT[P][M][W] statistics counter is created when first PM packet for loss measurement is received for PMF ID + MA identifier + window within a Reporting interval. Rx-STAT[P][M][W] statistics counter is deleted at expiry of current reporting interval after Rx-STAT[P][M][W] statistics counters are reported to collector.

Tx-STAT[P][M][W]: This 2 dimensional statistics counter is maintained at every MA. Where P stands for PMF ID and W stands for window ID. Tx- STAT[P][M][W] counter maintains the number of packets sent out for a given PMF ID + MA identifier + window. PMF ID is unique within a SFC Domain, for a given PMF ID there could be multiple Windows. Tx-STAT[P][M][W] statistics counter is created when first PM packet for loss measurement is sent for PMF ID + MA identifier + window within a Reporting interval. Rx-STAT[P][M][W] statistics counter is deleted at expiry of current reporting interval after Tx-STAT[P][M][W] statistics counters are reported to collector.

3.2 Initiating a Packet Loss Measurement

Measurement Controller programs the PM Instance at the classifier. Classifier starts the packet classification (based on the classification rule/policy). The packet classification policy may be customer/network/service specific. Classifier updates/encodes corresponding PM instance for classified packets for each PM schedule in PM context header.

3.3 Encapsulation of Classified Packets

For the classified packet, PM Context Header is prepared with following information

- Set the type class value to the IANA allocated PM class.
- Set the type value to the required packet loss measurement type.
- If type value = 0x1
    - o Encode the list of MA identifier that need to participate in Packet Loss Measurement.
- If Value = 0x2, 0x3, 0x4, 0x5
    - o No need to encode MA identifier, since the type dictates the involved participating MA
- Set the window identifier as the current running window number
- Encode the 32 bit globally unique PMF ID using the flow ID context header as defined in [I-D quinn-sfc-nsh-tlv].

3.4 Incoming Packets Processing at MA

On receiving the packet with NSH header following operations are carried out:

Step 1: Detection of PM context header in a packet, by verifying the PM TLV class as allocated by IANA.
(If not detected, move to step 6)

Step 2: Check if PM type field value is 1 to 5.
(If not move to step 6).

Step 3: If PM type value = 2 to 5 move directly to Step 5

Step 4: Check presence of self MA identifier in MA identifier List.
(If not present, move to step 6)

Step 5: Record the value of PMF ID and window ID; increment the value of statistics counter Rx-STAT[P][M][W] by 1. If statistics counter doesn’t exist, create it and initialize it with 1.

Step 6: Packet is sent for normal processing

3.5 Outgoing Packets Processing at MA

At outgoing port of MA following operations are carried out.

Step 1: Record the value of PMF ID and window ID; increment the value of statistics counter Tx-STAT[P][M][W] by 1. If statistics counter doesn't exist, create it and initialize it with 1.

Step 2: Packet is sent for normal processing

3.6 MA Reporting the statistics to Collector

Reporting timer will run on Each MA. Consistency of this timer should be ensured across the entire MA in the SFP, ensuring the same is out of scope of this document.

On expiry of this timer following information needs to be sent to the Collector.

- MA identifier
- PM Type Value
- Value of all the accumulated Tx-STAT[P][M][W] statistics counter along with the corresponding PMF ID and Window Id
- Value of all the accumulated Rx-STAT[P][M][W] statistics counter along with the corresponding PMF ID and window Id

MA may delete the Tx-STAT[P][M][W], Rx-STAT[P][M][W] after sending the same to collector.

3.7 Packet Loss Calculation at Collector

Collector accumulates the statistics counters per PMF per MA identifier per MA per window. On receipt of report from a MA for a PMF if it has statistics related for an already collected window, received statistics will be summed up, otherwise a new entry is created. Collector computes the packet loss using the accumulated statistics per PMF per MA per window.

Packet Loss between MA (for example from MA1 to MA2) = (MA1)Tx-STAT[P][M][W] - (MA2)Rx-STAT[P][M][W]

Packet Loss at MA = (MA)Tx-STAT[P][M][W] - (MA)Rx-STAT[P][M][W]

4 Security Considerations

No specific security considerations for this document

5 IANA Considerations

5.1 TLV Class

IANA is requested to allocate a new class value for performance measurement from "Network Service Header (NSH) Parameters" registry.

Value	Description	Reference
New	Performance Measurement	[SFC-PM-arch]

6. Acknowledgments

We would like to thank Nobin Mathew for his review and comments.

7 References

7.1 Normative References

[I-D.ietf-sfc-nsh] Quinn, P. and U. Elzur, "Network Service Header", draft-ietf-sfc-nsh-01 (work in progress), July 2015.

7.2 Informative References

[RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784 DOI 10.17487/RFC2784, March 2000, <http://www.rfc-editor.org/info/rfc2784>.

[RFC5226] Narten, T. and H. Alvestrand,"Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC7498] Quinn, P., Ed. and T. Nadeau,Ed.,"Problem Statement for Service Function Chaining", RFC 7498, DOI 10.17487/RFC7498, April 2015, <http://www.rfc-editor.org/info/rfc7498>.

[SFC-arch] Quinn, P., Ed. and J. Halpern, Ed., "Service Function Chaining (SFC) Architecture", 2014, <http://datatracker.ietf.org/doc/draft-quinn-sfc-arch>.

[SFC-PM-arch] Anil, Gaurav and Vinod., "Performance Measurement Architecture for SFC", 2015,

[SFC-PM-Delay] Anil, Gaurav and Vinod., "Packet Delay Measurement for SFC", 2015,

Authors' Addresses

Anil Kumar S N
Huawei Technologies India Pvt. Ltd,
Near EPIP Industrial Area,
Kundalahalli Village,
Whitefield,
Bangalore - 560037

EMail: anil.sn@huawei.com

Gaurav Agrawal
Huawei Technologies India Pvt. Ltd,
Near EPIP Industrial Area,
Kundalahalli Village,
Whitefield,
Bangalore - 560037

EMail: gaurav.agrawal@huawei.com

Vinod Kumar S
Huawei Technologies India Pvt. Ltd,
Near EPIP Industrial Area,
Kundalahalli Village,
Whitefield,
Bangalore - 560037

EMail: vinods.kumar@huawei.com