IPPM
Internet-Draft
Intended status: Informational
Expires: April 15, 2013

L. Sun
BUPT
F. Yu
Huawei Technologies
W. Wang
BUPT

October 12, 2012

Flow-based Performance Measurement
draft-sun-ippm-flowbased-pm-00

Abstract

The performance measurements of service flow are becoming significant important for administrators monitoring the fitness of the network. This memo defines an end-to-end flow-based performance measurement method, which is achieved by generating synthetic measurement packets, injecting them to the network and analyzing the statistics carried in the measurement packets.This measurement method can measure flow characteristics such as delay, ipdv (IP Packet Delay Variation) and packet loss.

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 http://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 April 15, 2013.

Copyright Notice

Table of Contents

1. Introduction

The IETF IP Performance Metrics (IPPM) working group has defined a series of standard metrics that can be applied to the quality, performance and reliability of Internet data delivery services. The WG has produced protocols to enable communication among test equipment that implements the one- and two-way metrics (OWAMP and TWAMP respectively).

This memo introduces a new measurement method which is called FPM. It continues as follows. Section 2 discusses the existing problems and puts forward the motivation of FPM. Section 3 introduces terminology, followed by the overview of the FPM in Section 4. Section 5 and Section 6 introduce connection control and measurement process of the FPM respectively. Section 7 describes the usage of metrics in FPM which are defined in the current IPPM working group. Section 8 describes some exceptions and handling. At last it introduces a use case, which describes the deployment, characteristics and applications of FPM.

2. Problems statement

The TWAMP protocol proposed by IPPM WG provides a simple and useful network performance measurement method. It aims at using a safe and effective way to measure the performance of the IP network. TWAMP uses TWAMP-Control protocol to initiate, start, and stop test sessions, making the measurement process with more flexibility and security. It uses TWAMP-Test protocol for the actual network test by injecting test packets into network, so that various properties of the network can be measured offline effectively. However, while TWAMP is able to achieve most network measurement situations, it does not work well in some cases on the performance testing for real time business.

In some cases, it needs to monitor the various time-varying performance indexes of the IP network, the performance measurement should be based on real service stream and reflect the real performance of the network. For measuring the performance of the real service stream, TWAMP has the following defects due to the limit of measurement parameters and its framework.

- TWAMP is mainly used to measure the performance of the network. It cannot be well applied to the real-time performance measurement of a particular or one kind of applications.

- In the case of real time measurement of network performance, if the test packets are sent too frequently, the network load will be

increased and application flows will be affected. Otherwise, if the number of test packets is small, the performance of the network cannot be reflected accurately by the measurement.

For example, for real time streaming media services such as IPTV and video conference, packets carry QoS parameters to ensure service quality for different application flows. Network needs to real time monitor the performance of these application flows, in order to adjust the allocation of resources in network according to the monitoring results in real time, thereby ensuring the QoS requirements of different applications. For the performance measurement of such business discussed above, TWAMP cannot meet all the requirements well as a result of the above defects.

For the problems discussed above, it is required to define a new measurement framework, which is able to meet the demand for real time measurement of application flows, and does not have much impact on the data flow itself. At the same time, this new measurement method will be able to meet the following goals of the IPPM measurement: guarantee the Service Level Agreement (SLA) provided to the customers, detect/locate the network performance defects, react in response to performance degradation or the failures promptly, and optimize the network resources utilization.

In the following section, we discuss the requirements of IP performance measurement in IP mobile backhaul network.

In mobile operator’s backhaul network, there must be a performance monitoring mechanism to check the traffic status in the network. With the status information, some strategies can be implemented on entities. For example, eNodeB can implement online congestion control and bandwidth adjustment strategy based on the performance monitoring result. Hence, IPPM mechanism is required to provide a reasonable estimate of the amount of delay, ipdv (IP Packet Delay Variation) and packet loss in the backhaul network connecting it to the GW.

In order to avoid adding superfluous traffic to the backhaul and leading to the increase of the load level in the network, it is necessary that the frequency of measurement packets generation is kept at a minimum. Moreover, these packets should not lead to an excessive computational overload on the eNodeB and the GW. In other words, the process of generation of these probe packets should be simple and must not overload the transport interface. The packets must be small and infrequent so as to not cause un-necessary overload on the backhaul bandwidth.

Applications or traffic in mobile backhaul network are divided into

multiple bearers with proper mobile QoS parameters (e.g. QCI). If the mobile network would manage bearers as QoS and applications, then the performance of backhaul is more like to be based on applications or QoS. The currently active measurement method (e.g. TWAMP) may be able to do flow-based measurement by specifying DSCP for the TWAMP-test packets. But it can not well support the online measurement and the length of test packet is changeless and not varying as the real service packets. The average performance indexes measured by the active measurement method may not be suitable in these cases.

A new measurement method can be applied into backhaul network, by deploying an end-to-end performance monitor on eNodeB to assist eNodeB to execute the congestion control and flow scheduling. Played as sender entity, eNodeB sends out the OAM packets periodically to trigger the other end (e.g. another eNodeB or an SGW) replying acknowledgement packets, then to estimate the delay, ipdv (IP Packet Delay Variation) and packet loss of each application flow by collecting and calculating status information.

3. Conventions and Terminology

3.1. Conventions Used in This Document

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 [RFC2119].

3.2. Terminology

FPM: Flow-based Performance Measurement

FM:Forward Monitoring

BR:Backward Reporting

4. Overview

4.1. Goals and Motivation

It is required to provide a reasonable estimation measurement of delay, ipdv (IP Packet Delay Variation) and packet loss in IP network (such as backhaul network). The above parameters are functions of time, which are stochastic in nature. Therefore, the mechanism is required to provide statistical condition estimations of the IP link status. Since measurement injects some OAM packets to the network, it is necessary that the frequency of packet generation is kept at a

minimum. Moreover, these packets should not lead to an excessive computational overload on the measure device. In other words, the generation process of these measurement packets should be simple and must not overload the transport interface. The packets must be small and infrequent so as not to cause unnecessary overload on the network bandwidth or influence the service running on the network.

4.2. Protocol overview

Firstly we make some statement for FPM. We define a measurement method that can be used in some scene. The method proposed here is an end-to-end measurement method over IP layer; it can be implemented under the tunnel mode of IPSec. Two types of logical entities are defined, the FPM Initiator and the FPM Responder. The FPM process consists of two parts: Connection control and Measurement Process.

During Connection control phase, the FPM initiator sends a request to the FPM Responder on a random port to set up the FPM connection activation. The FPM Responder SHOULD listen to a well-known port (This port number is introduced to be assigned by the IANA.). Second the FPM Responder responds with an ACK packet including some parameters based on the request. When the FPM Initiator receives the ACK, it will prepare for starting the measurement process.

After the measurement, FPM Initiator sends Connection Deactivation request packet called DEA to the FPM Responder. The FPM Responder sends DEA-ACK packets back to the FPM Initiator after it receives the DEA packets to stop the measurement.

During the measurement process, the FPM Initiator periodically generates Forward Monitor (FM) packets with the source and destination IP addresses, and other classification information (for example DSCP class) of the service packets , which are sent to the FPM Responder. The generation and transmission of FM packets can be periodical with a specific time interval, or a certain number of business packets should be sent between two contiguous FM packets. The FPM Responder receives the FM packets and sends Backward Reporting (BR) packets which are constructed according to the FM packets. The path performance such as the delay, ipdv (IP Packet Delay Variation) and loss rate etc. are calculates by the FPM Initiator according to the information in the BR packets.

The FM packets have the same source and destination IP addresses, even the same DSCP class in some cases with the business packets. So they are carried through the transport network just most like the business packets, and delay, ipdv(IP Packet Delay Variation) and packet loss encountered by them resembles the performance as seen by the packets of the actual business flows. The FM and BR packets used

in FPM are small enough to produce influence to actual service flow as little as possible.

Essential differences exist between FPM and IPPM WG-defined measurement, such as TWAMP and OWAMP. The solutions adopted in TWAMP and OWAMP are counting the information of measurement packets sent to network by Sender, and actively obtaining the measurement results. FPM is based on the running traffic of applications, and it collects the statistics of real business flow. Additional OAM packets are sent among business flow. Those OAM packets can be small and the inserted frequency can be lower. The OAM packets are used to carry flow/application statistics, which can be used to measure and estimate the business flow performance.

4.3. Logical Model

The role and definition of the logical entities and measurement packets in FPM are defined as follows.

FPM is an end-to-end measurement, so two logical entities are defined.

- FPM Initiator: FPM Initiator serves as the sending endpoint, and charges for generating and sending the request to initiate a FPM connection. It could also send FM packets to collect measurement data and generate statistical report.

- FPM Responder: FPM Responder serves as the data receiving endpoint, and charges for responding the request of initiating a link. It could also send back a BR packet to the sending endpoint once it receives the FM packet from the FPM Initiator.

One possible scenario of relationships between these roles is shown below.

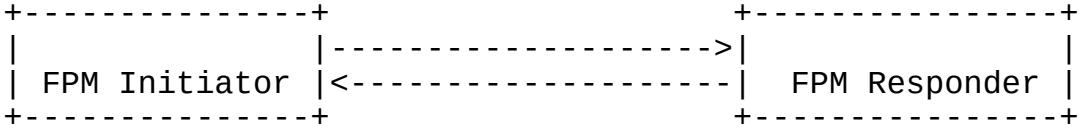


Figure 1: One possible relationship between FPM Initiator and FPM Responder

Note that the FPM Initiator can also serve as the data receiving endpoint, and the FPM Responder serves as the data sending endpoint. In this case the FM packets are sent by the FPM Responder and the BR packet is sent by the corresponding FPM Initiator. In later sections

the method is described for the first case. To avoid repetition, detail of this case is not described.

There are six types of packets in total, which include four types of control packets and two types of measurement packets.

Control packet:

- ACT: It is sent from the FPM Initiator to a specific UDP port on FPM Responder, carries parameters used in negotiation process when initiating a FPM connection.

- ACT-ACK: It is a response for ACT sent by the FPM Responder to the FPM Initiator.

- DEA: It is sent by the FPM Initiator to the FPM Responder for disconnecting the FPM connection.

- DEA-ACK: It is a response for DEA sent by the FPM Responder to the FPM Initiator.

Measurement packet:

- FM (Forward Monitoring): It is sent by the FPM Initiator. The format of FM packet payload as defined by this document will be shown below.

- BR (Backward Reporting): It is sent by the FPM Responder. The format of BR packet payload as defined by this document will be shown blow. It is a response for FM.

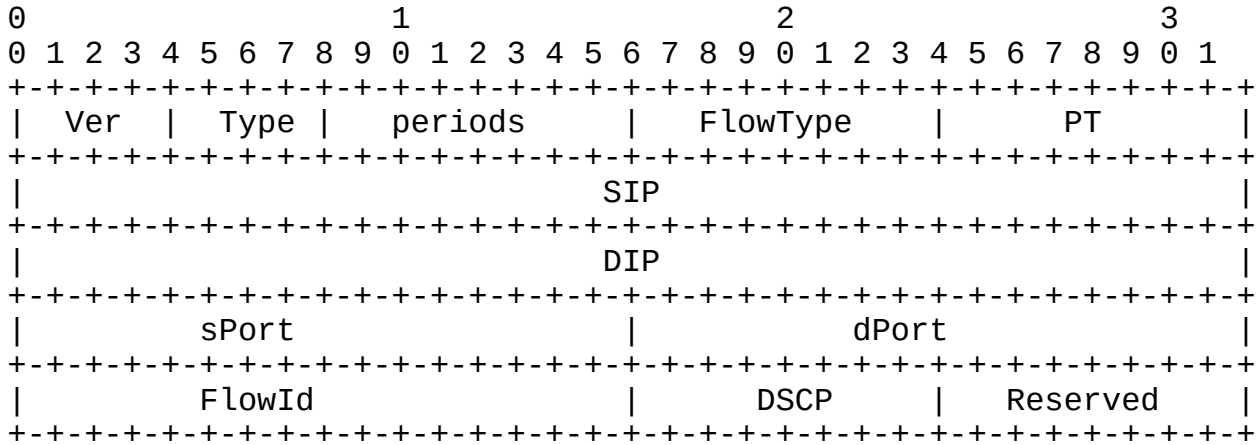
5. Connection Control

5.1. Connection Activation

In the FPM connection activation process, a Flow ID is assigned for a defined flow (the Flow ID is unique in a connection between the FPM Initiator and the FPM Responder). It should specify how to define the Flow corresponding to the measurement instance. Flow can be defined by different combinations of source IP address (SIP), destination IP address (DIP), protocol type (PT), DSCP, source port number (sPort) and destination port number (dPort). Three types of combinations are suggested: (SIP, DIP, PT), or (SIP, DIP, PT, DSCP) or (SIP, DIP, PT, sPort, dPort). The more the combinational dimensions are, the more fine-grained can be the monitoring of business flow.

Before starting the measurement, a connection should be established. When the FPM Initiator wants to start the measurement process, it enables the measurement capabilities to the FPM Responder by sending ACT packet to the specific UDP port on the FPM Responder. When the FPM Responder receives the ACT, it enables its measurement function and responses to the FPM Initiator with ACT-ACK packet. The connection activation process is finished after the FPM Initiator receiving the ACT-ACK packet from the FPM Responder, then the FPM Initiator can send FM packet after one cycle. The definition of flow, FlowID, and the sending period of FM packets must be consulted by two ends during the connection activation process.

The format of ACT packet is defined as follows:



Ver and Type existed in all packets in this memo indicate the version and type of packet. Type in these packets MUST be 0X1 indicates that this is an ACT packet.

Periods defined by FPM Initiator indicates the sending period of FM packets.

FlowType indicates how a flow is defined.0x0 in this field is for (SIP, DIP, PT, sPort, dPort), while 0x1 is for (SIP, DIP, PT, DSCP) and 0x2 is for (SIP, DIP, PT). The other values are not defined.

PT is the protocol type value of the service flow needed to be measured. It may be UDP, TCP, SCTP or other types.

SIP is the source IP address of the service flow, and DIP is the destination IP address of the service flow. SPort and DPort which are valid only when the flow is defined by (SIP, DIP, PT, sPort, dPort) indicate source/destination port number of the ACT packets.

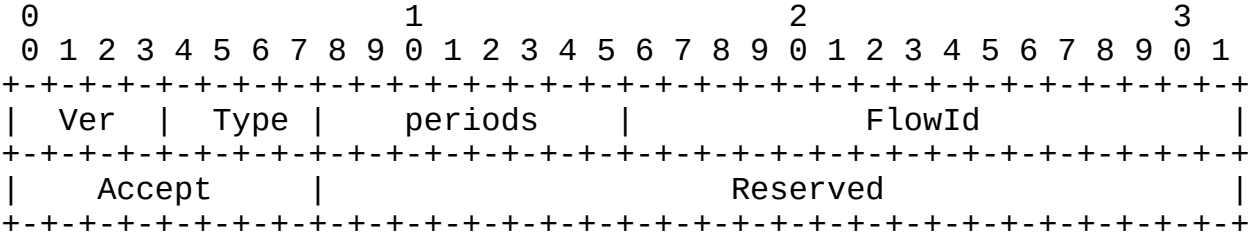
If the FlowType is not defined by (SIP, DIP, PT, sPort, dPort), this filed is 0xFF.

FlowId is the flow id assigned for the defined flow. It is defined by the FPM Initiator. The FlowId field in others control packets and measurement packets have the same meaning.

DSCP is valid only when the flow is defined by (SIP, DIP, PT, DSCP). It indicates the value of the DSCP filed in IP header of service flow.

Reserved is reserved for extensions in future and MUST be set to 0x0 currently.

The format of ACT-ACK packet is defined as follows:



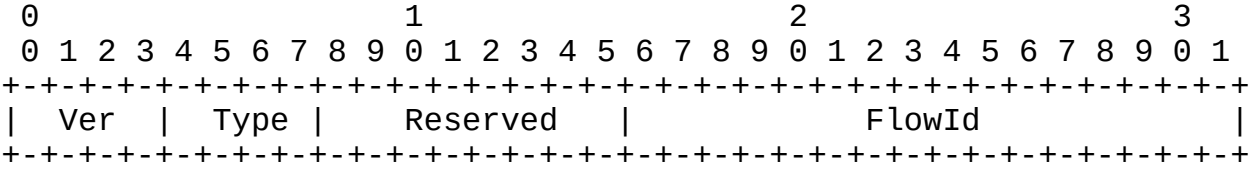
Type of 0X2 indicates ACT-ACK.

Accept is 0x0 means Connection Activation is OK. Accept is 0x01 means Connection Activation is failure and the reason is unspecified.

5.2. Connection Deactivation

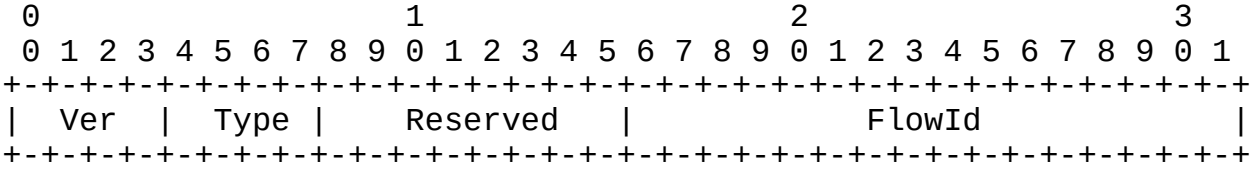
When the FPM Initiator wants to stop the measurement, it sends Connection Deactivation request packet called DEA to the FPM Responder. The FPM Responder sends DEA-ACK packets back to the FPM Initiator after it receives the DEA packets.

The format of DEA packet is defined as follows:



Type of 0X5 indicates DEA.

The format of DEA-ACK packet is defined as follows:



Type of 0X6 indicates DEA-ACK.

6. Measurement Process

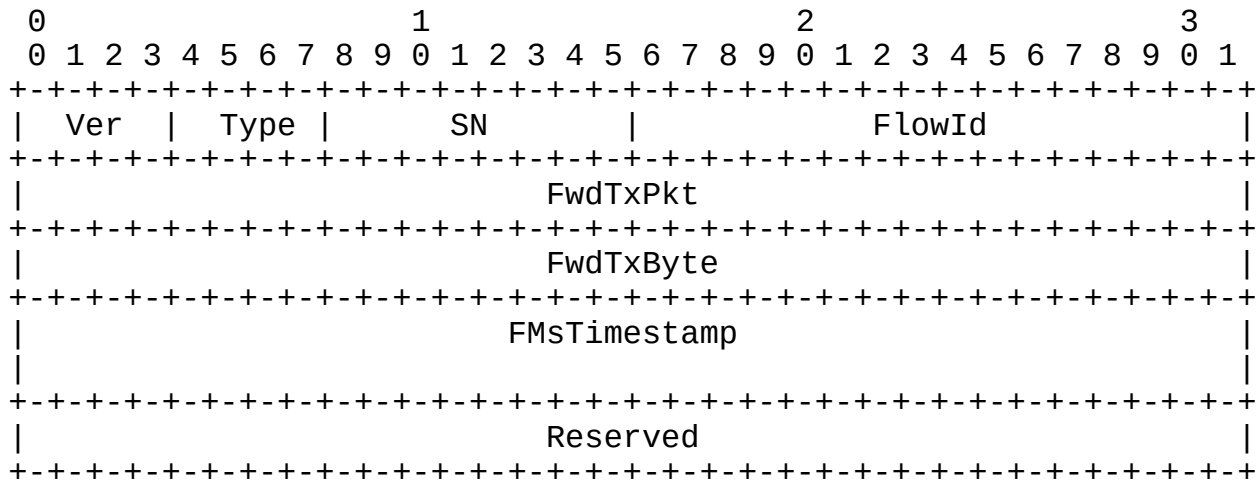
This section describes FPM Measurement process. It runs over UDP, and its packet header is constructed in accordance with the business packet except the source port number and destination port number. The destination port number is a well-known port number, and the source port number can be assigned a random port number. Its packets function is similar to the OAM packets, they can be small and the inserted frequency can be lower.

6.1. FPM Initiator behavior

In the measurement phase, FPM Initiator major responsibility is to structure and send FM measurement packet, as well as receive and process BR measurement packet.

When the connection is established successfully, the FPM Initiator sends FM packets according to the given time-interval. Regardless of any scheduling delays, each packet that is actually sent MUST have the best possible approximation of its real time of departure as its timestamp (in the packet).

The format of FM packet is defined as follows:



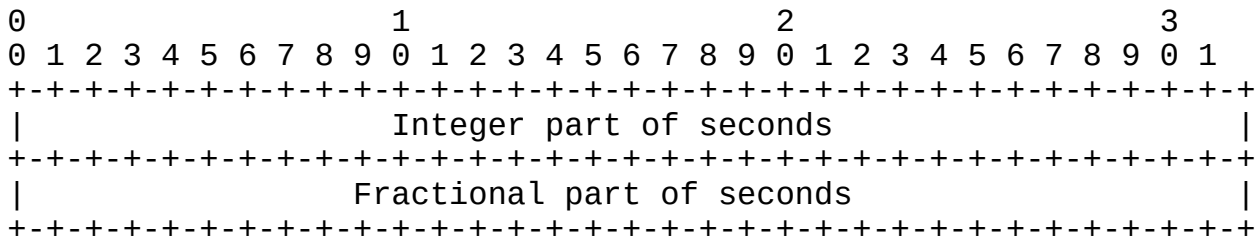
Type of 0X3 indicates FM.

SN is the sequence number of the flow, which distinguishes the different FM packets and indicates the correspondence between FM packets and BR packets. Each FPM flow SHOULD maintain a set of sequence numbers (SN).

FwdTxPkt is the accumulation of the number of the packets sent by the FPM Initiator. FwdTxByte is the accumulation of the number of bytes sent by the FPM Initiator. In order to determine the value of the fields of FwdTxPkt and FwdTxByte, the FPM Initiator maintains two counters, SPN and SBN, for each FPM flow that is incremented every time a business packet is sent. When the FM packets are to be sent, the FwdTxPkt and FwdTxByte are set to the then value of the counters respectively.

FMsTimestamp is the timestamp when the FPM Initiator sends the first bit of the FM packets.

The format of the FMsTimestamp is the same as in [RFC5905] and is as follows: the first 32 bits represent the unsigned integer number of seconds elapsed since 0h on 1 January 1900; the next 32 bits represent the fractional part of a second that has elapsed since then. The timestamp follows the above format in the below sections.

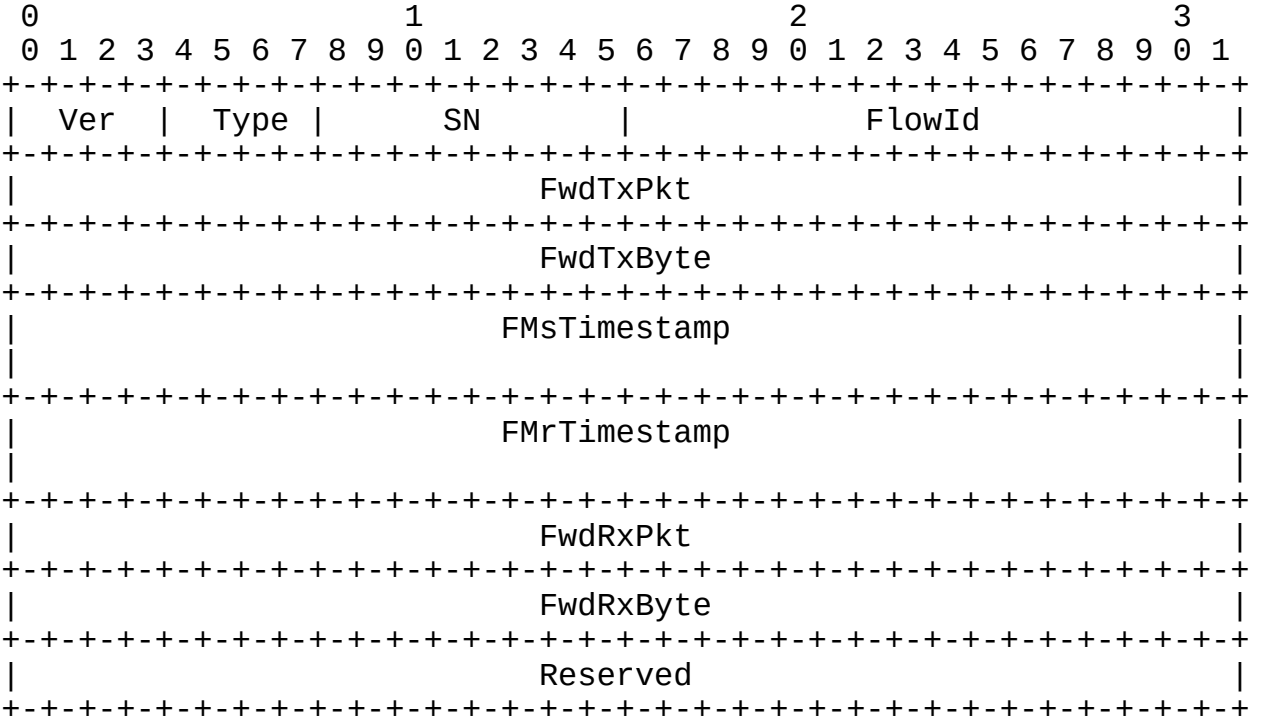


6.2. FPM Responder behavior

FPM requires the FPM Responder to transmit a packet to the FPM Initiator in response to each FM packet it receives.

When the FPM Responder receives a FM packet, it copies the value of FwdTxPkt, FwdTxByte and Timestamp in FM packet into the corresponding fields of the BR packet, and sets the fields of Sender Timestamp, FwdRxPkt and FwdRxByte and sends the BR packet.

The format of BR packet is defined as follows:



Type of 0X4 indicates BR.

SN is copied from the SN field of the corresponding FM packet.

The FwdTxPkt and FwdTxByte are copied from the corresponding FM packet.

FwdRxPkt is the accumulation of the number of the packets received by the FPM Responder.

FwdRxByte is the accumulation of the number of bytes received by the FPM Responder.

In order to determine the value of the fields of FwdRxPkt and FwdRxByte, the FPM Responder maintains two counters, RPN and RBN, for each FPM flow that is incremented every time a business packet is received. When the BR packets are to be sent, the FwdRxPkt and FwdRxByte are set to the then value of the counters respectively.

FMsTimestamp is copied from the Timestamp field of the FM packets; FMrTimestamp is the timestamp when the FPM Responder receives the last bit of the FM packets. The format of the timestamp is the same as in FM packets.

Note that the FPM Initiator could start multiple measurement engines; each engine is corresponding to an active logical path (with a different Flow). These measurement engines operate in parallel, and send FM packets with the flow id of the logical path, collect the corresponding BR packets, and maintain the collected statistical values.

7. Metrics

FPM method can measure most of the Metrics defined by IPPM WG. We assume that the reader is familiar with IPPM working group document, some terms in these documents may be used as described below.

[RFC2679] describes the one-way delay metrics between the IP hosts. Delay is dT means that Src sent the first bit of a Type-P packet to Dst at time T and that Dst received the last bit of that packet at time T+dT[RFC2679]. In FPM, FMsTimestamp in FM packet is the timestamp when the FPM Initiator sent the first bit of the FM packet, and FPM Responder records the timestamp when the FPM Responder received the last bit of the FM packets. Assuming that time in both ends are synchronous, one-way delay in one measurement can be derived through FMrTimestamp-FMsTimestamp.

[RFC2679]also describes a pseudo-random Poisson sampling method for sampling T between the designated T0 and Tf (T0 and Tf is the sampling time boundary value). FPM can sample the set of results measured in FPM Initiator, and the sampling method can be the pseudo-

random Poisson sampling or other methods. Error handling and other operations are described in [RFC2679].

[RFC2680] defines the one-way packet loss metrics between the IP hosts. If the packet can reach the destination host, the data loss value is 0. If the packet is lost during transmission, the data loss value is 1[RFC2680]. The host records whether the business packet is lost or not during the measurement cycle and it can calculate the unidirectional IP packet loss for this period of time. FPM uses this method to get statistics of the business packet loss. In the measurement process, FPM Initiator uses a counter to count the actual number of packets sent by it. FPM Responder records whether business packet has arrived or not, if the packet reaches the FPM Responder, business packet loss value is 0; if the packet is lost during transmission, the business packet loss value is 1. FPM Responder cumulates the loss value, and calculates the number of packets actually received. The above parameters, carried by measurement packets, are exchanged between both sides, used to calculate packet loss and loss rate in FM Initiator ultimately.

As described above, measurement packet only needs to carry statistics information of both sides in the FPM. The measurement packet size and the transmission frequency are relatively small, so FPM will not cause too much impact on the original business.

Similarly, the FPM methods can also measure metrics defined in [RFC3393] and [RFC4737].

Note that the statistics is carried in the IP layer. They are calculated before packet fragmentation at the FPM Initiator and after packet reassembly at the FPM Responder. If both the FPM Initiator and the FPM Responder support IPSec, the parameter statistics, including number of bytes/packets, Delay and ipdv (IP Packet Delay Variation), are carried before IPSec process is executed. If IPHC (IP Header Compression) is used at the two ends, the parameter statistics should be carried before IPHC.

7.1. Example of loss rate

Using the statistics of loss data, we can calculate the value of loss rate. The flowing is an example.

When the dth BR packet is received at the FPM Initiator, the loss rate plr based on the dth BR packet and (d-1)th BR packet is calculated as:

$$plrd = \frac{(SPN(d)-SPN(d-1))-(RPN(d)-RPN(d-1))}{SPN(d)-SPN(d-1)}$$

(SPN(d)-SPN(d-1))indicates the number of service packets sent by the FPM Initiator during dth measurement, and (RPN(d)-RPN(d-1)) indicates the actual number of service packets received by the FPM Responder during dth measurement.

The loss rate needs to be aggregated over the reporting interval. Let’s assume that N BR packets were received during the dth reporting interval. Therefore, the packet loss rate for that interval can be calculated as:

$$PLRd = \frac{1}{N} * \sum_{d=1}^{N} plrd$$

8. Exception Handling

8.1. FM/BR Packet Loss

In some cases the FM or BR packet may be lost in transit, then no statistics can be obtained from this round of measurement.

So the loss rate of the mth measurement can be calculated as:

$$plrd = \frac{(SPN(m)-SPN(n))-(RPN(m)-RPN(n))}{SPN(m)-SPN(n)}$$

where m is the SN of the BR packet currently received and n is the SN of the latest BR received.

8.2. Packet Reordering

In the receive side if the received packets are out of order, the FM packet may arrive earlier than the last service packet sent before it, or later than the first service packet sent after it. Then statistical error of packet loss will be result in.

There are several reasons for packet reordering. When a network node

receives a fragmented IP packet, it has to reassemble the datagram and the extra time spent on the IP fragment reassembly may cause packet reordering; Some load sharing schemes for network (e.g. ECMP, ML-PPP) may create multipath for packets, which can also cause packet reordering; Multi-core CPU processing and multi-threading of packets in the sender and receiver may also lead to packet reordering.

In the simplest case that data transmits along a single path, DSCP can be used to classify the flow in order to avoid the packet reordering.

Note that the packet loss calculation is based on sample statistic, and by increasing the monitoring period, the error caused by the occasional packet reordering can be smoothed.

9. Use Case

This section describes a typical scene using the measurement method. The wireless mobile backhaul networks based on IP, share the available capacity between the connected eNodeBs. Compared to the traditional SDH/ATM transport network, in IP-RAN, the data transfer speed is unstable and data transfer is lacks of QoS guarantee and there is no perfect testing method on packet loss, delay and ipdv (IP Packet Delay Variation). So it is necessary for the nodes in the RAN side to detect the network quality of the connection between RNC and NodeB or eNodeB and SAE.

Take the eNodeB and SAE for example; in order to make sure that the amount of generated traffic is aligned with the available capacity, it is important that the eNodeB probes the backhaul network to determine the actual delay, jitter and packet loss encountered by typical packets. The proposed method in this document can be used to detect the IP Performance of the connections between the eNB and S-GW.

As shown below, FPM Initiator is deployed in eNodeB, and FPM Responder is deployed in S-GW.

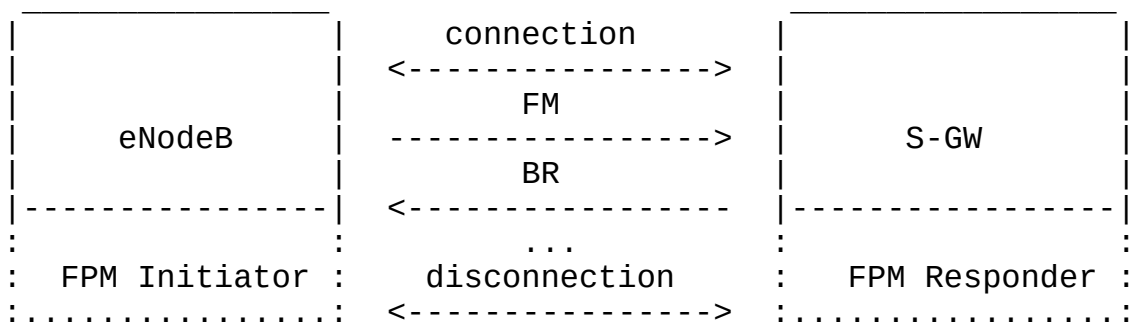


Figure 2: Example of FPM in backhaul network

At the eNodeB, FM packets are generated periodically with the source and destination IP addresses, and DSCP class. At the S-GW, after receiving the FM packets, BR packets are constructed. They are then forwarded back to the eNodeB.

We sent a similar packet of OAM, packet size and the transmission frequency is relatively small, so FPM will not cause too much impact on the original business between eNodeB and S-GW. Since the measurement packet is constructed according to the business packet, the network path of measurement packet and business packet is the same (Tunneling is used for the data transmission between eNodeB and S-GW, the parameter statistics of FPM should be carried before the tunnel. Measurement packet and business packet are encapsulated into a same tunnel and they are passed in the same path). The data obtained through FPM can represent the performance of the business flows between the eNodeB and the S-GW accurately.

Upon receiving the BR packets at the logical port the eNodeB exactly knows the current congestion extent in transport network. The bandwidth of the logical port is reduced if congestion is detected according to the measurement result; otherwise, the bandwidth is increased slowly.

10. Security Considerations

To be defined.

11. IANA Considerations

The destination port number of the newly defined packets for measurement needs to be assigned by the IANA.

12. Acknowledgments

The authors gratefully acknowledge reviews and contributions from Peter McCann.

The authors would like thank Xiangyang Gong and Xirong Que for their technical guidance towards to this draft.

The authors would like to thank Yuehui Ding for editing problem statement.

13. References

13.1. Normative Reference

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2679] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Delay Metric for IPPM", RFC 2679, September 1999.

[RFC2680] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Packet Loss Metric for IPPM", RFC 2680, September 1999.

[RFC5905] Mills, D., Martin, J., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

13.2. Informative References

[RFC2330] Paxson, V., Almes, G., Mahdavi, J., and M. Mathis, "Framework for IP Performance Metrics", RFC 2330, May 1998.

[RFC3393] Demichelis, C. and P. Chimento, "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)", RFC 3393, November 2002.

[RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, September 2006.

[RFC4737] Morton, A., Ciavattone, L., Ramachandran, G., Shalunov, S., and J. Perser, "Packet Reordering Metrics", RFC 4737, November 2006.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J.

Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, October 2008.

Authors' Addresses

Lishun Sun
Beijing University of Posts and Telecommunications
Xitucheng road 10
Haidian District, Beijing 100876
P. R. China

Email: lishunsun@Gmail.com

Fang Yu
Huawei Technologies
Huawei Building, Q20 No.156 Beiqing Rd.Z-park
Haidian District, Beijing 100095
P. R. China

Email: grace.yufang@huawei.com

Wendong Wang
Beijing University of Posts and Telecommunications
Xitucheng road 10
Haidian District, Beijing 100876
P. R. China

Email: wdwang@bupt.edu.cn