

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: January 8, 2017

G. Fioccola  
Telecom Italia  
A. Clemm  
Cisco Systems  
M. Cociglio  
Telecom Italia  
M. Chandramouli  
Cisco Systems  
A. Capello  
Telecom Italia  
July 7, 2016

**Alternate Marking Extension to Active Measurement Protocol  
draft-fioccola-ippm-alt-mark-active-00**

**Abstract**

This document describes how to extend the existing Active Measurement Protocol, in order to implement alternate marking methodology detailed in [[I-D.ietf-ippm-alt-mark](#)]. The extension for Two-Way Active Measurement Protocol (TWAMP) [RFC 5357](#) [[RFC5357](#)] and One-way Active Measurement Protocol (OWAMP) [RFC 4656](#) [[RFC4656](#)] will be considered. This proposal defines a simplified mechanism with benefits to the metric precision and computational load. Hybrid measurements are also enabled.

**Requirements Language**

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](#)].

**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 January 8, 2017.

## Copyright Notice

Copyright (c) 2016 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 (<http://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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

|                      |   |                    |
|----------------------|---|--------------------|
| <a href="#">1.</a>   | Introduction . . . . .                              | <a href="#">2</a>  |
| <a href="#">2.</a>   | Description of the method . . . . .                 | <a href="#">3</a>  |
| <a href="#">2.1.</a> | Packet loss measurement . . . . .                   | <a href="#">4</a>  |
| <a href="#">2.2.</a> | Delay measurement . . . . .                         | <a href="#">5</a>  |
| <a href="#">2.3.</a> | Delay variation measurement . . . . .               | <a href="#">6</a>  |
| <a href="#">3.</a>   | Hybrid measurement . . . . .                        | <a href="#">6</a>  |
| <a href="#">4.</a>   | Protocol Extension overview . . . . .               | <a href="#">6</a>  |
| <a href="#">4.1.</a> | Control Phase . . . . .                             | <a href="#">8</a>  |
| <a href="#">4.2.</a> | Test Phase . . . . .                                | <a href="#">8</a>  |
| <a href="#">4.3.</a> | Calculation Phase . . . . .                         | <a href="#">9</a>  |
| <a href="#">5.</a>   | Open Issues . . . . .                               | <a href="#">9</a>  |
| <a href="#">5.1.</a> | Extension of TWAMP/OWAMP Control Protocol . . . . . | <a href="#">10</a> |
| <a href="#">5.2.</a> | Extension of TWAMP/OWAMP Test Protocol . . . . .    | <a href="#">10</a> |
| <a href="#">6.</a>   | IANA Considerations . . . . .                       | <a href="#">10</a> |
| <a href="#">7.</a>   | Security Considerations . . . . .                   | <a href="#">10</a> |
| <a href="#">8.</a>   | Acknowledgements . . . . .                          | <a href="#">10</a> |
| <a href="#">9.</a>   | References . . . . .                                | <a href="#">10</a> |
| <a href="#">9.1.</a> | Normative References . . . . .                      | <a href="#">10</a> |
| <a href="#">9.2.</a> | Informative References . . . . .                    | <a href="#">11</a> |
|                      | Authors' Addresses . . . . .                        | <a href="#">11</a> |

## [1.](#) Introduction

The Two-Way Active Measurement Protocol (TWAMP), specified in [RFC 5357](#) [[RFC5357](#)] adds two-way or round-trip measurement capabilities to the One-way Active Measurement Protocol (OWAMP) specified in [RFC 4656](#) [[RFC4656](#)]. OWAMP can be used bi-directionally to measure one-way metrics in both directions between two network elements. The TWAMP measurement architecture is usually comprised of two hosts with



specific roles, and this allows for some protocol simplifications, making it an attractive alternative in some circumstances. Another example is Cisco's Service-Level Assurance Protocol (Cisco's SLA Protocol) [RFC 6812](#) [[RFC6812](#)], a Performance Measurement protocol that has been widely deployed. Details are explained in [[I-D.fioccola-ippm-rfc6812-alt-mark-ext](#)].

One technique for passive performance measurements is described in [[I-D.ietf-ippm-alt-mark](#)]. This technique involves marking production flows as they traverse the network, then analyzing flow data associated with those marked flows. Passive measurements are very accurate in that they measure actual production traffic. However, there are scenarios in which passive measurements are not an option. For example, there may be no suitable flows currently occurring between pairs of nodes to be measured, or traffic may be tunneled and not be accessible to marking. Furthermore active measurements permit a precise control of the monitored traffic than passive measurements. So in such cases, active measurements using synthetic test traffic need to be considered.

This document specifies how to implement active measurement with the same technique described in [[I-D.ietf-ippm-alt-mark](#)]. Instead of time stamping test traffic, test traffic is marked and measurements occur by analyzing resulting flow data. There are some key aspects of the mechanism described in this document to be considered:

- o Improve metric precision: the packet timestamp can be take in an more efficient way because it is not inserted within the Test packet.
- o Reduce computational load: no sequence numbers and no timestamps within the Test packets.
- o Enable hybrid measurements thanks to the Alternate Marking.

## **[2.](#) Description of the method**

In order to perform packet loss, delay and jitter measurements on a traffic flow, different approaches exist. The method proposed consists in counting and timestamping the packets sent from one end, the packets received on the other end, and compare the two values. Therefore the devices performing the measurement have to refer exactly to the same set of packets. So the flow is virtually spit in consecutive blocks by coloring the packets so that the packets belonging to the same block will have the same color, whilst consecutive blocks will have different colors. Each change of color represents a sort of auto-synchronization signal that guarantees the



consistency of measurements taken by different devices along the path.

This approach, called Alternate Marking method, is efficient both for passive performance monitoring and for active performance monitoring. In this document we describe the implementation for Active Measurement.

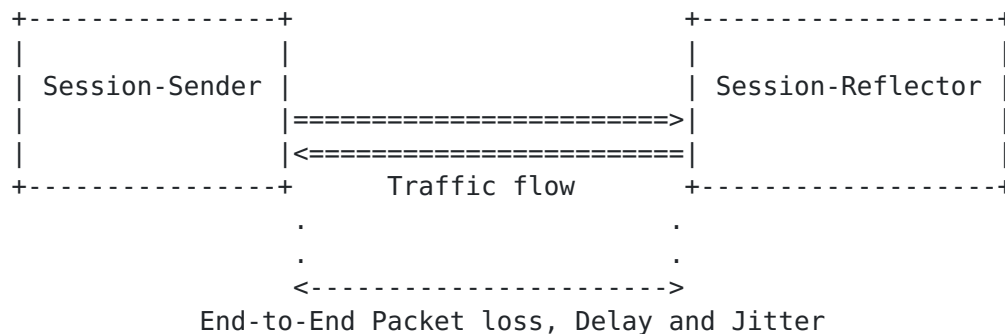


Figure 1: Available measurements

Previous Figure represents two end points (Session-Sender and Session-Reflector) that exchange two equal data flows in both direction. The data flows start and end together. Packets are colored and the color changes every marking interval. The method can be used to measure packet loss, delay and jitter.

## 2.1. Packet loss measurement

The basic idea is to virtually split traffic flows into consecutive blocks: each block represents a measurable entity unambiguously recognizable by all network devices along the path. By counting the number of packets in each block and comparing the values measured by Sender and Reflector, it is possible to measure packet loss occurred in any single block between the two end points.

A simple way to create the blocks is to "color" the traffic (two colors are sufficient) so that packets belonging to different consecutive blocks will have different colors. Whenever the color changes, the previous block terminates and the new one begins. The number of packets in each block depends on the criterion used to create the blocks: if the color is switched after a fixed number of packets, then each block will contain the same number of packets (except for any losses); but if the color is switched according to a fixed timer, then the number of packets may be different in each block depending on the packet rate.



## **2.2. Delay measurement**

The same principle used to measure packet loss can be applied also to one-way delay measurement. There are two alternatives, shown below:

- o Delay for each packet: For active measurement two alternate marking data flows are generated in both direction, so the alternation of colors can be used as a time reference to calculate the delay. Whenever the color changes (that means that a new block has started) an end point can store the timestamps of all packets of the new block. The timestamps can be compared with the timestamps of the same packets on the other end point to compute packet delay. This method for measuring the delay is sensitive to out of order reception of packets. In order to overcome this problem between packets there should be a security time gap to avoid out of order issues. If the packet rate exchanged between the two end points is adequate each end points can store all the timestamp of the block and the packet delay can be computed for all the packets of the block, included minimum, maximum, average and median delay values.
- o Average delay: A different approach, based on the concept of average delay, can be take in account for active measurement. The average delay is calculated by considering the average arrival time of the packets within a single block. The network device locally stores a timestamp for each packet received within a single block: summing all the timestamps and dividing by the total number of packets received, the average arrival time for that block of packets can be calculated. By subtracting the average arrival times of the two end points it is possible to calculate the average delay. This method is robust to out of order packets and also to packet loss (only a small error is introduced). Moreover, it greatly reduces the number of timestamps (only one per block for each end point) that have to be collected and transmitted for the calculation. On the other hand, it only gives one measure for the duration of the block, and it doesn't give the minimum, maximum and median delay values. [RFC 6703](#) [[RFC6703](#)] recommends to report both median and average delay in order to obtain additional information about the distribution. But the same procedure of the average delay is not applicable to median delay because the median is not a linear operator. So the average delay could be considered as a light measurement because the calculation is achieved by exchanging only the average timestamp for each colored block (without exchanging all the timestamps). For this reason the average delay is not the main technique, but a secondary option in case we have to save computational resources.



By summing the one-way delay measurements of the two directions of a path, it is also possible to measure the two-way delay (round-trip delay).

In brief, there are three choices to compute delay for active measurement:

- o The two end points could store all packets timestamps in both directions. At the end of the period all timestamps are exchanged. In this way, delay is calculated for each packet.
- o The two end points calculate only the average timestamp that is exchanged at the end of the period. In this way only the average delay is calculated.
- o The two end points sent packets with a specified and shared traffic profile and each end point could make its own calculation (data are not exchanged so it is not so accurate, but it depends on hardware and software capabilities).

Note: How data and timestamps are exchanged is outside the scope of this document.

### **2.3. Delay variation measurement**

Similarly to one-way delay measurement, the method can also be used to measure the inter-arrival jitter. The alternation of colors can be used as a time reference to measure delay variations. The inter-arrival jitter can be easily derived from one-way delay measurement, by evaluating the delay variation of consecutive samples.

The concept of average delay can also be applied to delay variation, by evaluating the variation of average interval between consecutive packets of the flow.

## **3. Hybrid measurement**

In order to have both end to end measurements and intermediate measurements (hybrid measurements) Sender and Reflector exchanges traffic flows and apply alternate marking over these flows. In the intermediate points artificial traffic is managed in the same way as real traffic and measured as specified before.

## **4. Protocol Extension overview**

The Alternate Marking extension to Active Measurement Protocol like OWAMP or TWAMP, consists of three distinct phases, Control Phase, Test Phase and Calculation Phase.



The Control Phase is the first phase of message exchanges and forms the base protocol. This phase establishes the identity of the Sender and provides information for the Test Phase.

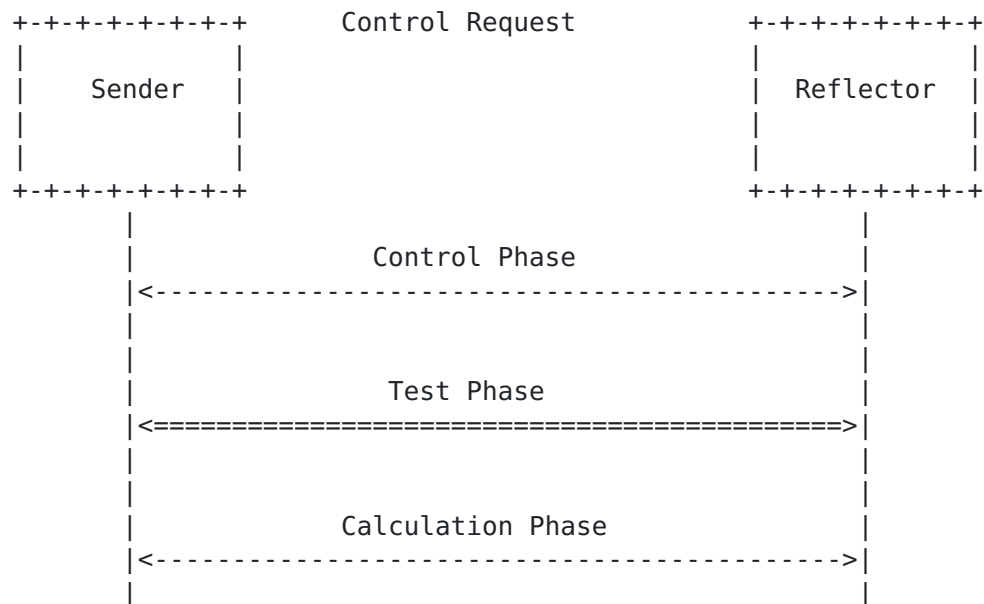
The Test Phase forms the second phase and is comprised of an exchange of two equal alternate marking data flows between Sender and Reflector. Sender and Reflector generate test traffic and apply marking, no traffic is reflected and no timestamping is added to packets.

The Calculation Phase is introduced "ad hoc" for Alternate Marking implementation because it does not exist in other Active Measurement Protocol. After test execution there are some alternatives to compute packet loss, delay and delay variation:

- o Local assessment: Sender initiates a Calculation Request message and Reflector sends back a Calculation Response message. Sender and Reflector, upon receipt test traffic, create data structure with timestamped records then computes service level metrics from that data structure. Let's call this data structure the test receipt.
- o Central assessment: A "central" entity (e.g. a controller) compares the test receipt collected by the Reflector with data structure obtained from the Sender, then computes the service levels by means of comparing.
- o Local assessment with reference recording: Both sender and receiver play out the same test traffic. Assessment is done locally not by computing metrics over the test receipt, but by "overlaying" the original with the one that was received and computing the delta.

The number and frequency with which messages are sent SHOULD be controlled by configuration on the Sender element, along with the waiting time for a Control Response.

The following sequence diagram depicts the message exchanges:



To utilize existing Active Measurement Protocol, some extensions are needed. The Sender indicates that alternate marking techniques are to be used and that traffic is going to be marked. Likewise, it can indicate to the Reflector to not simply reflect the marked traffic, but to generate a separate stream of marked test traffic back to the sender. The marking pattern will be conveyed (including the markings to be used and duration of the marking intervals). The implementation of measurements involves analyzing the marked traffic as needed. Conveying of results of the analysis of observed traffic occurs through separate means, not specified here.

#### 4.1. Control Phase

The Control Phase consists of agreement between Sender and Reflector. Only an extension to the existing protocols is needed. Please refer to the guidelines defined in [Section 3](#) of OWAMP [RFC 4656](#) [[RFC4656](#)] TWAMP [RFC 5357](#) [[RFC5357](#)] or [RFC 6812](#) [[RFC6812](#)].

#### 4.2. Test Phase

Upon successfully completing the Control Phase, the second phase of the protocol, the Test Phase, is initiated. In the Test Phase the Sender sends a stream of measurement messages. The measurement message stream consists of packets/frames that are spaced a configured number of milliseconds.

The Measurement messages are simplified in comparison to OWAMP [RFC 4656](#) [[RFC4656](#)] TWAMP [RFC 5357](#) [[RFC5357](#)] or [RFC 6812](#) [[RFC6812](#)]. In



particular the fields that can be removed are: Sender Timestamp, Receive Timestamp, Sequence Number.

The format of the Measurement messages is the same for the exchange in both directions, that is when sent from the Sender to the Reflector and from the Reflector to the Sender.

Note: Marking field can be chosen in two ways for OWAMP [RFC 4656](#) [[RFC4656](#)] and TWAMP [RFC 5357](#) [[RFC5357](#)]: marking Packet Padding or MBZ fields.

Note: Marking field can be chosen for [RFC 6812](#) [[RFC6812](#)] in two ways: marking UDP payload or marking IPv4 header.

Note: No timestamp, No sequence number. The two data flows are independent.

### **[4.3.](#) Calculation Phase**

As mentioned above, the Calculation Phase is introduced "ad hoc" for Alternate Marking implementation because it does not exist in OWAMP [RFC 4656](#) [[RFC4656](#)] TWAMP [RFC 5357](#) [[RFC5357](#)] or [RFC 6812](#) [[RFC6812](#)]. After test execution there are some alternatives to compute packet loss, delay and delay variation:

- o Local assessment: Sender initiates a Calculation Request message and Reflector sends back a Calculation Response message. Sender and Reflector, upon receipt test traffic, create data structure with timestamped records then computes service level metrics from that data structure. Let's call this data structure the test receipt).
- o Central assessment: A "central" entity (e.g. a controller) compares the test receipt collected by the Reflector with data structure obtained from the Sender, then computes the service levels by means of comparing.
- o Local assessment with reference recording: Both sender and receiver play out the same test traffic. Assessment is done locally not by computing metrics over the test receipt, but by "overlaying" the original with the one that was received and computing the delta.

## **[5.](#) Open Issues**



### **5.1. Extension of TWAMP/OWAMP Control Protocol**

to be added

### **5.2. Extension of TWAMP/OWAMP Test Protocol**

to be added

## **6. IANA Considerations**

IANA Considerations to be added.

## **7. Security Considerations**

Security Considerations to be added.

## **8. Acknowledgements**

Mauro Cociglio and Giuseppe Fioccola worked in part on the Leone research project, which received funding from the European Union Seventh Framework Programme [FP7/2007-2013] under grant agreement number 317647.

## **9. References**

### **9.1. Normative References**

- [I-D.fioccola-ippm-rfc6812-alt-mark-ext]  
Fioccola, G., Clemm, A., Cociglio, M., Chandramouli, M., and A. Capello, "Alternate Marking Extension to Cisco SLA Protocol [RFC6812](#)", [draft-fioccola-ippm-rfc6812-alt-mark-ext-01](#) (work in progress), March 2016.
- [I-D.ietf-ippm-alt-mark]  
Capello, A., Cociglio, M., Fioccola, G., Castaldelli, L., and A. Bonda, "Alternate Marking method for passive performance monitoring", [draft-ietf-ippm-alt-mark-00](#) (work in progress), June 2016.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", [RFC 4656](#), DOI 10.17487/RFC4656, September 2006, <<http://www.rfc-editor.org/info/rfc4656>>.

- [RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarez, "A Two-Way Active Measurement Protocol (TWAMP)", [RFC 5357](#), DOI 10.17487/RFC5357, October 2008, <<http://www.rfc-editor.org/info/rfc5357>>.
- [RFC6812] Chiba, M., Clemm, A., Medley, S., Salowey, J., Thombare, S., and E. Yedavalli, "Cisco Service-Level Assurance Protocol", [RFC 6812](#), DOI 10.17487/RFC6812, January 2013, <<http://www.rfc-editor.org/info/rfc6812>>.

## **9.2. Informative References**

- [RFC6703] Morton, A., Ramachandran, G., and G. Maguluri, "Reporting IP Network Performance Metrics: Different Points of View", [RFC 6703](#), DOI 10.17487/RFC6703, August 2012, <<http://www.rfc-editor.org/info/rfc6703>>.

### Authors' Addresses

Giuseppe Fioccola  
Telecom Italia  
Via Reiss Romoli, 274  
Torino 10148  
Italy

Email: [giuseppe.fioccola@telecomitalia.it](mailto:giuseppe.fioccola@telecomitalia.it)

Alexander Clemm  
Cisco Systems  
170 West Tasman Drive  
San Jose 95134  
USA

Phone: 1-408-526-4000  
Email: [alex@cisco.com](mailto:alex@cisco.com)

Mauro Cociglio  
Telecom Italia  
Via Reiss Romoli, 274  
Torino 10148  
Italy

Email: [mauro.cociglio@telecomitalia.it](mailto:mauro.cociglio@telecomitalia.it)



Mouli Chandramouli  
Cisco Systems

Email: moulchan@cisco.com

Alessandro Capello  
Telecom Italia  
Via Reiss Romoli, 274  
Torino 10148  
Italy

Email: alessandro.capello@telecomitalia.it