IPPM Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 15, 2018

X. Min
D. Zhanwei
ZTE

October 12, 2017

TWAMP Extensions for Direct Loss Measurement
draft-xiao-ippm-twamp-ext-direct-loss-01

Abstract

This document describes an optional extension for Two-Way Active Measurement Protocol (TWAMP) allowing direct loss measurement of IP traffic with the TWAMP-Test protocol.

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 April 15, 2018.

Copyright Notice

Table of Contents

1. Introduction

The Two-Way Active Measurement Protocol (TWAMP) [RFC5357] is an extension of the One-Way Active Measurement Protocol (OWAMP) [RFC4656]. The TWAMP is a well-defined protocol which is widely used for measurement of two-way or round-trip metrics, in addition to the one-way metrics of OWAMP.

When TWAMP or OWAMP is used for measurement of metric loss, it actually measures the loss of test packets, so it's a kind of "synthetic" loss measurement. In some cases, considering the IP traffic loss characteristics of short-time burst loss, it's expected to get more accurate loss measurement results when measuring the direct loss of IP traffic instead of test packets.

To address this, this document describes an optional and simple feature for TWAMP, which allows TWAMP-Test protocol to be used for direct loss measurement of IP traffic.

1.1. Conventions Used in This Document

1.1.1. Terminology

DSCP: Differentiated Services Code Point

IPPM: IP Performance Metrics

TWAMP: Two-Way Active Measurement Protocol

OWAMP: One-Way Active Measurement Protocol

UDP: User Datagram Protocol

1.1.2. Requirements Language

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.

2. TWAMP-Control Extension

TWAMP connection establishment follows the procedure defined in Section 3.1 of [RFC4656] and Section 3.1 of [RFC5357] where the Modes field is used to identify and select specific communication capabilities. At the same time, the Modes field is recognized and used as an extension mechanism [RFC6038]. The new feature requires a new flag, Direct Loss Measurement flag, to identify the ability of both Session-Sender and Session-Reflector to perform direct loss measurement, and to support the new Session-Sender packet format and the new Session-Reflector packet format in the TWAMP-Test protocol. See Section 6 for details on the assigned bit position.

2.1. Connection Setup with Direct Loss Measurement Mode

The Server sets the Direct Loss Measurement flag in the Modes field of the Server Greeting message to indicate its capability and willingness to perform it. If the Control-Client agrees to perform direct loss measurement on some or all test sessions invoked with this control connection, it MUST set the Direct Loss Measurement flag in the Modes field in the Setup Response message.

3. TWAMP-Test Extensions

The TWAMP-Test protocol is similar to the OWAMP [RFC4656] test protocol with the exception that the Session-Reflector transmits test packets to the Session-Sender in response to each test packet it receives. TWAMP, see Section 4 of [RFC5357], defines two additional test packet formats for packets transmitted by the Session-Reflector. The appropriate format depends on the security mode chosen. The new mode specified in this document adds counter(s) of IP traffic packets into each test packet format.

When the Server and Control-Client have agreed to use the direct loss measurement mode during control connection setup, then the Session-

Sender and the Session-Reflector SHOULD all conform to the requirements of that mode, as identified below.

3.1. Sender Test Packet Format and Content

Formats of the test packet transmitted by the Session-Sender in unauthenticated, authenticated, and encrypted modes have been defined in Section 4.1.2 of [RFC4656] (as indicated in Section 4.1.2 of [RFC5357]). For the Session-Sender that supports direct loss measurement, these formats are displayed in Figures 1 and 2.

For unauthenticated mode:

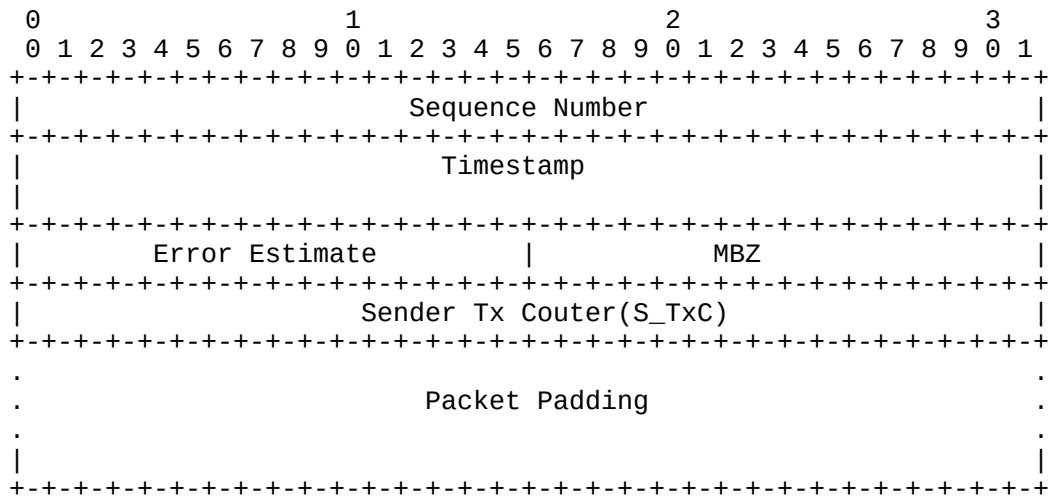


Figure 1: Session-Sender Test Packet Format with direct loss measurement in Unauthenticated Mode

For authenticated and encrypted modes:

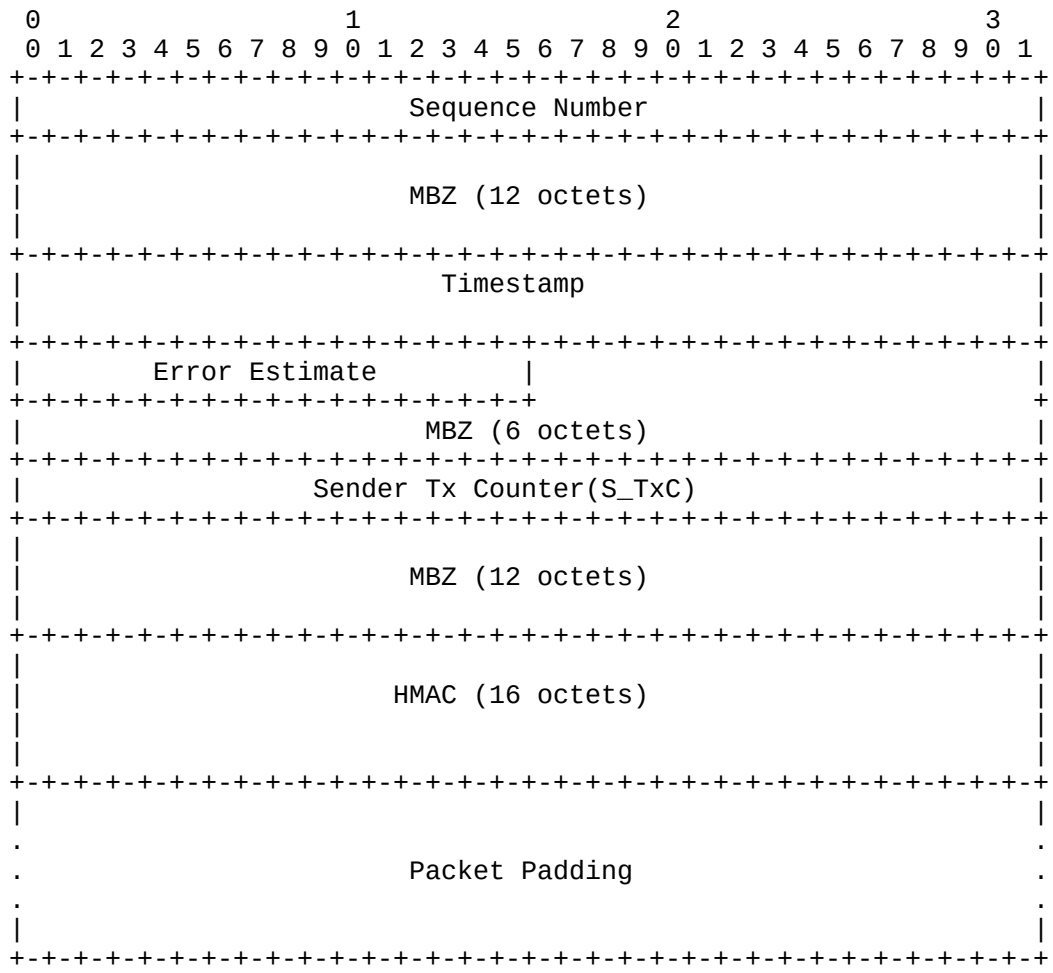


Figure 2: Session-Sender Test Packet Format with Direct Loss Measurement in Authenticated and Encrypted Modes

The Sender Tx Counter (S_TxC) is set to the number of IP packets of the particular monitored flow transmitted towards the Reflector. Section 4 provides operational guide on how to determine the scope of IP traffic packets that need to be counted. Note that the Sender test packets are not counted.

In authenticated and encrypted modes, the S_TxC is followed by a new 12 octets MBZ (MUST be zero) field to make it 16-octet aligned, which is required for authentication and encryption.

The intention of embedding S_TxC in the Session-Sender test packets is for the Session-Sender to calculate direct loss of IP traffic, and the loss calculation algorithm is described in Section 3.3.

The new direct loss measurement mode defined in this document and the two extended TWAMP modes defined in [RFC6038] can be selected simultaneously.

When the Symmetrical Size mode defined in [RFC6038] is also selected, S_TxC SHOULD be embedded in the Session-Sender Packet formatted in Section 5.1.4 of [RFC6038], with the same position as depicted in Figure 1.

When the Reflect Octets mode defined in [RFC6038] is also selected, S_TxC SHOULD be embedded in the Session-Sender Packet formatted in Section 5.1.2 of [RFC6038], with the same position as depicted in Figure 1.

When both the Symmetrical Size mode and the Reflect Octets mode are also selected, S_TxC SHOULD be embedded in the Session-Sender Packet formatted in Section 5.1.5 of [RFC6038], with the same position as depicted in Figure 1.

3.2. Reflector Test Packet Format and Content

Formats of the test packet transmitted by the Session-Reflector in unauthenticated, authenticated, and encrypted modes have been defined in Section 4.2.1 of [RFC5357]. For the Session-Reflector that supports direct loss measurement, these formats are displayed in Figures 3 and 4.

For unauthenticated mode:

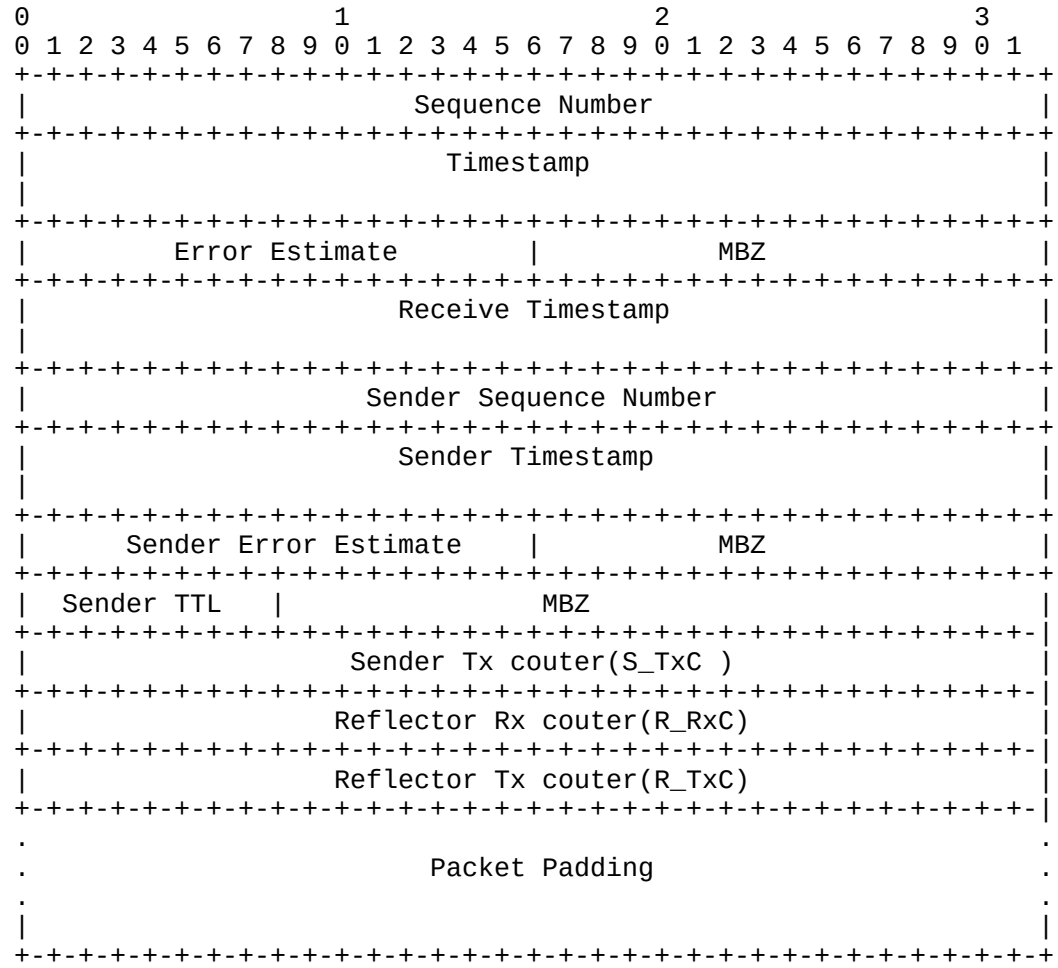
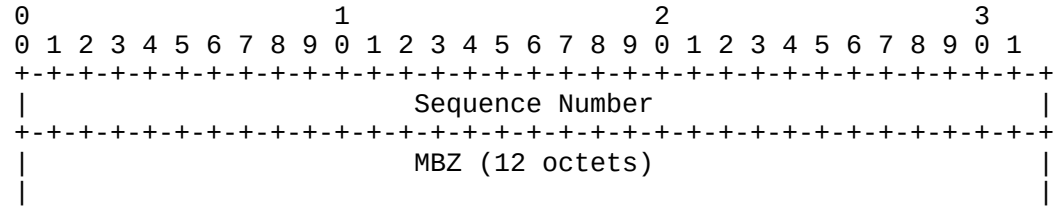
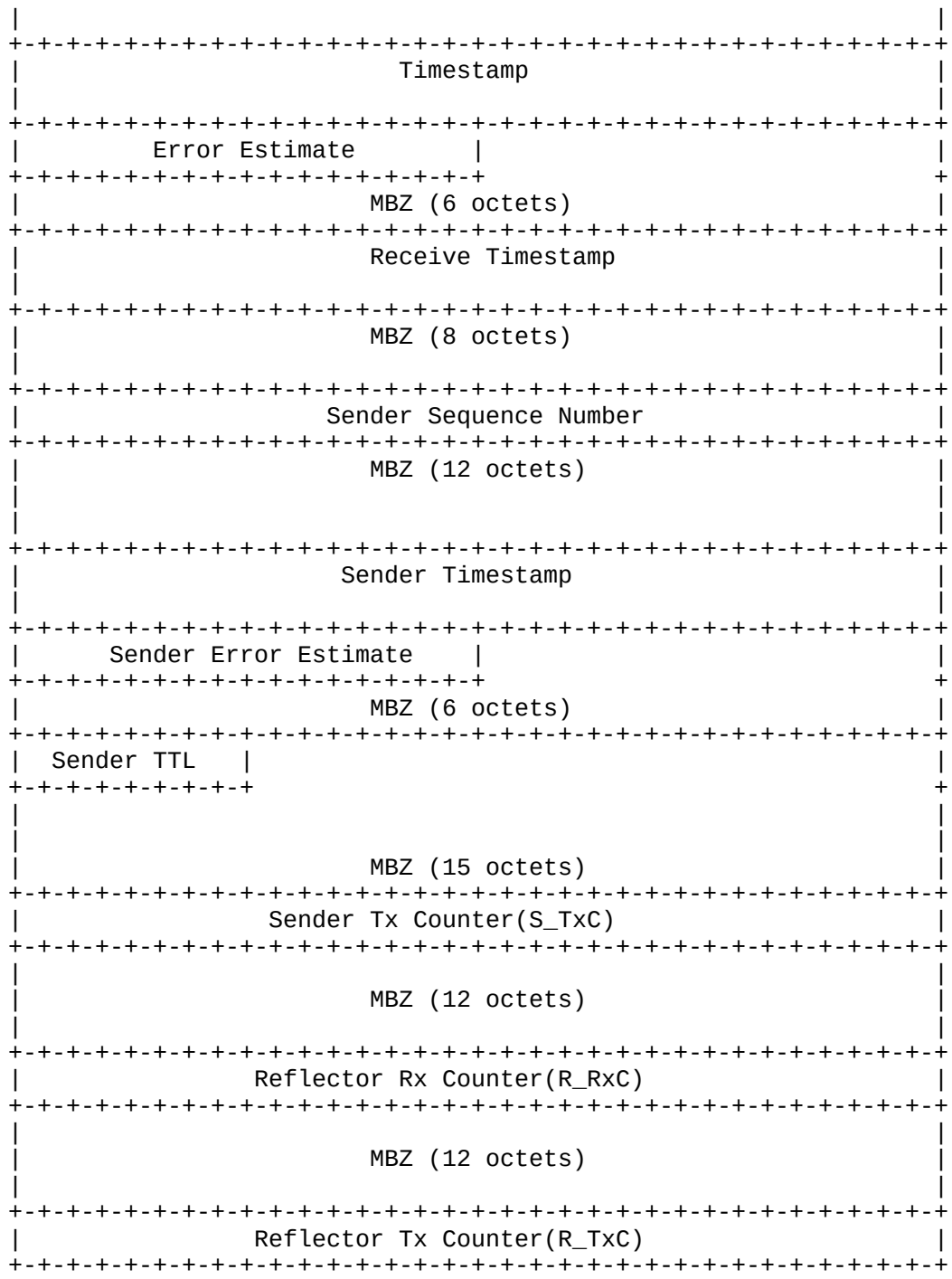


Figure 3: Session-Reflector Test Packet Format with direct loss measurement in Unauthenticated Mode

For authenticated and encrypted modes:




Timestamp
Error Estimate
MBZ (6 octets)
Receive Timestamp
MBZ (8 octets)
Sender Sequence Number
MBZ (12 octets)
Sender Timestamp
Sender Error Estimate
MBZ (6 octets)
Sender TTL
MBZ (15 octets)
Sender Tx Counter(S_TxC)
MBZ (12 octets)
Reflector Rx Counter(R_RxC)
MBZ (12 octets)
Reflector Tx Counter(R_TxC)

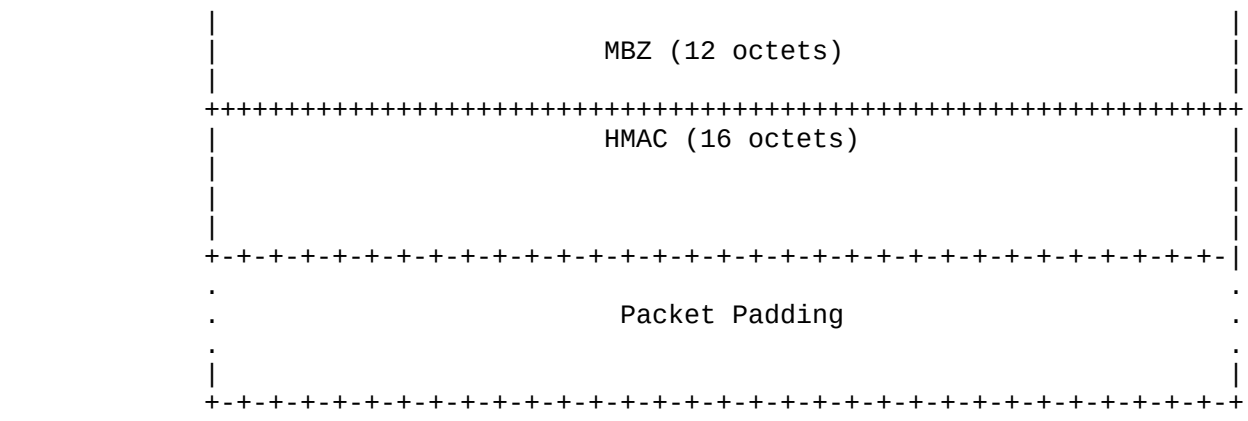


Figure 4: Session-Reflector Test Packet Format with Direct Loss Measurement in Authenticated and Encrypted Modes

The Sender Tx Counter (S_TxC) is copied from the received Sender Test Packet.

The Reflector Rx Counter (R_RxC) is set to the number of IP traffic packets received by the Reflector. Section 4 provides operational guide on how to determine the scope of IP traffic packets that need to be counted. Note that the Sender test packets are not counted.

The Reflector Tx Counter (R_TxC) is set to the number of IP traffic packets transmitted towards the Sender. Section 4 provides operational guide on how to determine the scope of IP traffic packets that need to be counted. Note that the Reflector test packets are not counted.

In authenticated and encrypted modes, the S_TxC, R_RxC and R_TxC are respectively followed by a new 12 octets MBZ (MUST be zero) field to make it 16-octet aligned, which is required for authentication and encryption.

The intention of embedding S_TxC, R_RxC and R_TxC in the Session-Reflector test packets is for the Session-Sender to calculate direct loss of IP traffic, and the loss calculation algorithm is described in Section 3.3.

When the Symmetrical Size mode defined in [RFC6038] is also selected, basing on what's specified in Section 5.2.2 of [RFC6038], the Session-Reflector packet format would follow Figure 3.

When the Reflect Octets mode defined in [RFC6038] is also selected, S_TxC, R_RxC and R_TxC SHOULD be embedded in the Session-Reflector Packet formatted in Section 5.2.1 of [RFC6038], with the same position as depicted in Figure 3.

When both the Symmetrical Size mode and the Reflect Octets mode are also selected, S_TxC, R_RxC and R_TxC SHOULD be embedded in the Session- Reflector Packet formatted in Section 5.2.1 of [RFC6038], with the same position as depicted in Figure 3.

3.3. Traffic Loss Calculation

Upon receiving a Reflector Test Packet, the Session-Sender uses the following values to make loss calculation:

o Received S_TxC, R_RxC and R_TxC values embedded in Reflector Test Packet and local counter S_RxC value at the time this Reflector Test Packet was received. These values are represented as S_TxC[n], R_RxC[n], R_TxC[n], and S_RxC[n], where n is the reception time of the current Reflector Test Packet.

o Previous Received S_TxC, R_RxC and R_TxC values embedded in Reflector Test Packet and local counter S_RxC value at the time the previous Reflector Test Packet was received. These values are represented as S_TxC[n-1], R_RxC[n-1], R_TxC[n-1], and S_RxC[n-1], where n-1 is the reception time of the previous Reflector Test Packet.

The formulas for calculating the far-end loss, near-end loss, far-end loss rate and near-end loss rate are as following:

o Far-end loss: F_Loss[n-1,n] = (S_TxC[n]-S_TxC[n-1])-(R_RxC[n]-R_RxC[n-1])

o Near-end loss: N_Loss[n-1,n] = (R_TxC[n]-R_TxC[n-1])-(S_RxC[n]-S_RxC[n-1])

o Far-end loss rate: F_LossRate[n-1,n] = F_Loss[n-1,n]/(S_TxC[n]-S_TxC[n-1])

o Near-end loss rate: N_LossRate[n-1,n] = N_Loss[n-1,n]/(R_TxC[n]-R_TxC[n-1])

Here far-end means the direction from the Session-Sender to the Session-Reflector and near-end means the direction from the Session-Reflector to the Session-Sender.

4. Operational Guide

In order to make meaningful loss measurement, in general, the scope of IP traffic packets that need to be counted, i.e. the IP traffic packets counting rules, should be provisioned before starting Test Sessions, and the provisioned arguments usually include ingress port, source IP address, destination IP address, IP DSCP and UDP port number. For the scenarios where the exact source/destination IP address and IP DSCP of IP traffic can be known, such as mobile backhaul, the Test Packets should use the same source/destination IP address and IP DSCP as IP traffic, and it shall result in more accurate measurements.

5. Security Considerations

Use of direct loss measurement in a test session does not appear to introduce any additional security threat to hosts that communicate with TWAMP as defined in [RFC5357]. The security considerations that apply to any active measurement of live networks are relevant here as well. See the Security Considerations sections in [RFC4656] and [RFC5357].

6. IANA Considerations

In the TWAMP-Modes registry defined in [RFC5618], a new Direct Loss Measurement Capability is requested from IANA as follows:

Bit Pos	Description	Semantics Definition	Reference
10	Direct Loss Measurement Capability	Section 2	This Document

Table 1: New Direct Loss Measurement Capability

7. Acknowledgements

The authors would like to thank Greg Mirsky and Guo Jun for their valuable comments.

8. 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>.

[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, <https://www.rfc-editor.org/info/rfc4656>.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, DOI 10.17487/RFC5357, October 2008, <https://www.rfc-editor.org/info/rfc5357>.

[RFC5618] Morton, A. and K. Hedayat, "Mixed Security Mode for the Two-Way Active Measurement Protocol (TWAMP)", RFC 5618, DOI 10.17487/RFC5618, August 2009, <https://www.rfc-editor.org/info/rfc5618>.

[RFC6038] Morton, A. and L. Ciavattone, "Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features", RFC 6038, DOI 10.17487/RFC6038, October 2010, <https://www.rfc-editor.org/info/rfc6038>.

[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

Xiao Min
ZTE
Nanjing
CN

Phone: +86 25 88016576
Email: xiao.min2@zte.com.cn

Dou Zhanwei
ZTE
Nanjing
CN

Phone: +86 25 52874656
Email: dou.zhanwei@zte.com.cn