Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 25, 2013

C. Bi
STTRI
A. Clark
Telchemy
G. Hunt
Unaffiliated
Q. Wu
Huawei
G. Zorn, Ed.
Network Zen

October 22, 2012

RTCP XR Report Block for Loss Concealment Metric Reporting
draft-ietf-xrblock-rtcp-xr-loss-conceal-03.txt

Abstract

This document defines an RTCP XR Report Block that allows the reporting of loss concealment metrics primarily for audio applications of RTP.

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 25, 2013.

Table of Contents

1. Introduction

1.1. Standards 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].

1.2. Loss Concealment Report Block

This draft defines a new block type to augment those defined in Friedman, et al. [RFC3611] for use in a range of RTP applications.

At any instant, the audio output at a receiver may be classified as either 'normal' or 'concealed'. 'Normal' refers to playout of audio payload received from the remote end, and also includes locally generated signals such as announcements, tones and comfort noise. Concealment refers to playout of locally-generated signals used to mask the impact of network impairments or to reduce the audibility of jitter buffer adaptations.

The new block type provides metrics for actions taken by the receiver to mitigate the effect of packet loss and packet discard. Specifically, the first metric (On-Time Playout Duration) reports the duration of normal playout of data which the receiver obtained from the sender's stream. A second metric (Loss Concealment Duration) reports the total time during which the receiver played out media data which was manufactured locally, because the sender's data for these periods was not available due to packet loss or discard. A similar metric (Buffer Adjustment Concealment Duration) reports the duration of playout of locally-manufactured data replacing data unavailable due to adaptation of an adaptive de-jitter buffer. Further metrics (Playout Interrupt Count and Mean Playout Interrupt Size) report the number of times normal playout was interrupted, and the mean duration of these interruptions.

Loss Concealment Duration and Buffer Adjustment Concealment Duration are reported separately because buffer adjustment is typically arranged to occur in silence periods and so may have very little impact on user experience, whilst loss concealment may occur at any time.

The metric belongs to the class of transport-related terminal metrics defined in Wu, et al. [I-D.ietf-avtcore-monarch].

1.3. RTCP and RTCP XR Reports

The use of RTCP for reporting is defined in Schulzrinne, et al. [RFC3550]. Friedman, Cacares & Clark [RFC3611] define an extensible structure for reporting using an RTCP Extended Report (XR). This draft defines a new Extended Report block that MUST be used as specified in RFC 3550 and RFC 3611.

1.4. Performance Metrics Framework

Clark & Claise [RFC6390] provides guidance on the definition and specification of performance metrics. Wu, et al. [I-D.ietf-avtcore-monarch] provides guidelines for RTCP XR report block formats. The report block defined in this document is in accordance with those guidelines.

1.5. Applicability

This metric is primarily applicable to audio applications of RTP. EDITOR'S NOTE: are there metrics for concealment of transport errors for video?

2. Loss Concealment Block

2.1. Report Block Structure

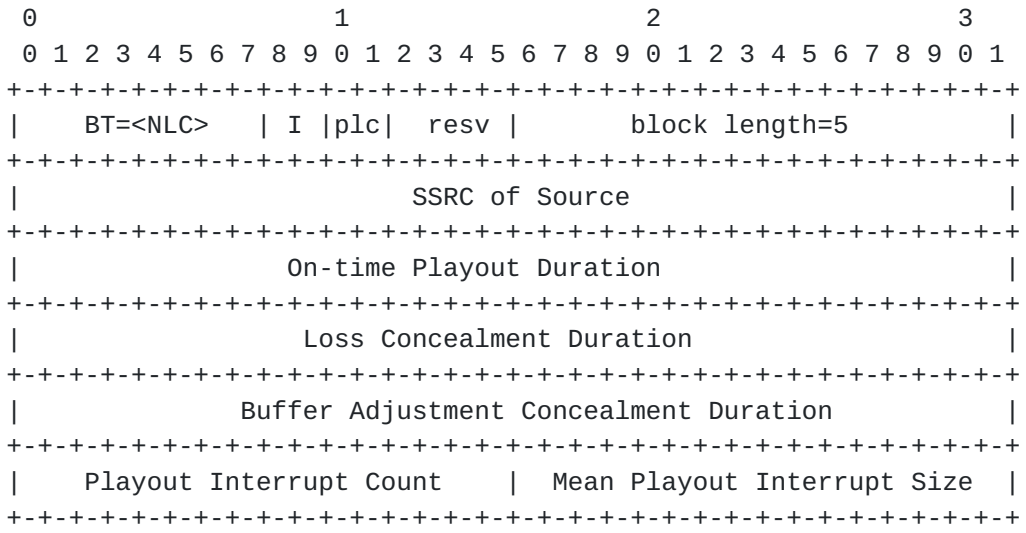

Figure 1: Structure of the Loss Concealment Metrics Block

2.2. Definition of Fields in Loss Concealment Report Block

Block type (BT): 8 bits

A Loss Concealment Metrics Report Block is identified by the constant <NLC>.

[Note to RFC Editor: please replace <NLC> with the RTCP XR block type allocated by IANA for this block.]

Interval Metric flag (I): 2 bits

This field is used to indicate whether the delay metrics are sampled, interval or cumulative metrics, that is, whether the reported values applies to the most recent measurement interval duration between successive metrics reports (I=10) (the interval duration) or to the accumulation period characteristic of cumulative measurements (I=11) (the cumulative duration) or is a sampled instantaneous value (I=01) (sampled value).

Packet Loss Concealment Method (plc): 2 bits

This field is used to identify the packet loss concealment method in use at the receiver, according to the following scheme:

00 = silence insertion

01 = simple replay, no attenuation

10 = simple replay, with attenuation

11 = enhanced

Reserved (resv): 4 bits

These bits are reserved. They MUST be set to zero by senders and SHOULD be ignored by receivers.

block length: 16 bits

The length of this report block in 32-bit words, minus one. For the Loss Concealment block, the block length is equal to 5.

SSRC of source: 32 bits

As defined in Section 4.1 of RFC 3611.

On-time Playout Duration (ms): 32 bits

'On-time' playout is the uninterrupted, in-sequence playout of valid decoded audio information originating from the remote endpoint. This includes comfort noise during periods of remote talker silence if voice activity detection (VAD) is in use, and locally generated or regenerated tones and announcements.

An equivalent definition is that on-time playout is playout of any signal other than those used for concealment.

On-time playout duration MUST include both speech and silence intervals, whether VAD is used or not. This duration is reported in millisecond units.

If the measured value exceeds 0xFFFFFFFD, the value 0xFFFFFFFE SHOULD be reported to indicate an over-range measurement. If the measurement is unavailable, the value 0xFFFFFFFF SHOULD be reported.

Loss Concealment Duration (ms): 32 bits

The duration, in milliseconds, of audio playout corresponding to loss-type concealment.

Loss-type concealment is reactive insertion or deletion of samples in the audio playout stream due to effective frame loss at the audio decoder. "Effective frame loss" is the event in which a frame of coded audio is simply not present at the audio decoder when required. In this case, substitute audio samples are generally formed, at the decoder or elsewhere, to reduce audible impairment.

If the measured value exceeds 0xFFFFFFFD, the value 0xFFFFFFFE SHOULD be reported to indicate an over-range measurement. If the measurement is unavailable, the value 0xFFFFFFFF SHOULD be reported.

Buffer Adjustment Concealment Duration (ms): 32 bits

The duration, in milliseconds, of audio playout corresponding to buffer adjustment concealment, if known.

If the measured value exceeds 0xFFFFFFFD, the value 0xFFFFFFFE SHOULD be reported to indicate an over-range measurement. If the measurement is unavailable, the value 0xFFFFFFFF SHOULD be reported.

Buffer adjustment concealment is proactive or controlled insertion or deletion of samples in the audio playout stream due to jitter buffer adaptation, re-sizing or re-centering decisions within the endpoint.

Because this insertion is controlled, rather than occurring randomly in response to losses, it is typically less audible than loss-type concealment. For example, jitter buffer adaptation events may be constrained to occur during periods of talker silence, in which case only silence duration is affected, or sophisticated time-stretching methods for insertion/deletion during favorable periods in active speech may be employed.

Concealment events which cannot be classified as buffer adjustment MUST be classified as loss concealment.

Playout Interrupt Count: 16 bits

The number of interruptions to normal playout which occurred during the reporting period.

If the measured value exceeds 0xFFFD, the value 0xFFFE SHOULD be reported to indicate an over-range measurement. If the measurement is unavailable, the value 0xFFFF SHOULD be reported.

Mean Playout Interrupt Size (ms): 16 bits

The mean duration, in ms, of interruptions to normal playout which occurred during the reporting period.

If the measured value exceeds 0xFFFD, the value 0xFFFE SHOULD be reported to indicate an over-range measurement. If the measurement is unavailable, the value 0xFFFF SHOULD be reported.

3. SDP Signaling

The use of the Session Description Protocol (SDP) [RFC4566] for signaling the use of XR blocks is described in RFC 3611. XR blocks MAY be used without prior signaling.

This section augments the SDP attribute "rtcp-xr" defined in Section 5.1 of RFC 3611 by providing an additional value of "xr-format" to signal the use of the report block defined in this document.

rtcp-xr-attrib = "a=" "rtcp-xr" ":" [xr-format *(SP xr-format)] CRLF

(defined in RFC 3611)

xr-format =/ xr-conceal-block

xr-conceal-block = "loss-conceal"

4. IANA Considerations

New block types for RTCP XR are subject to IANA registration. For general guidelines on IANA considerations for RTCP XR, refer to RFC 3611.

4.1. New RTCP XR Block Type value

This document assigns the block type value <NLC> in the IANA "RTCP XR Block Type Registry" to the "Loss Concealment Metrics Block".

[Note to RFC Editor: please replace <NLC> with the RTCP XR block type assigned by IANA for this block.]

4.2. New RTCP XR SDP Parameter

This document also registers a new parameter "loss-conceal" in the "RTCP XR SDP Parameters Registry".

4.3. Contact Information for Registrations

The contact information for the registrations is:

Alan Clark (alan.d.clark@telchemy.com)

2905 Premiere Parkway, Suite 280
Duluth, GA 30097
USA

5. Security Considerations

It is believed that this proposed RTCP XR report block introduces no new security considerations beyond those described in RFC 3611. This block does not provide per-packet statistics so the risk to confidentiality documented in Section 7, paragraph 3 of RFC 3611 does not apply.

6. Acknowledgements

The authors gratefully acknowledge the comments and suggestions made by Bruce Adams, Philip Arden, Amit Arora, Bob Biskner, Kevin Connor, Claus Dahm, Randy Ethier, Roni Even, Jim Frauenthal, Albert Higashi, Tom Hock, Shane Holthaus, Paul Jones, Rajesh Kumar, Keith Lantz, Mohamed Mostafa, Amy Pendleton, Colin Perkins, Mike Ramalho, Ravi Raviraj, Albrecht Schwarz, Tom Taylor, and Hideaki Yamada.

7. References

7.1. Normative References

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

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[RFC3611] Friedman, T., Caceres, R., and A. Clark, "RTP Control Protocol Extended Reports (RTCP XR)", RFC 3611, November 2003.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

7.2. Informative References

[I-D.ietf-avtcore-monarch] Wu, W., Hunt, G., and P. Arden, "Guidelines for Use of the RTP Monitoring Framework", draft-ietf-avtcore-monarch-22 (work in progress), September 2012.

[RFC6390] Clark, A. and B. Claise, "Guidelines for Considering New Performance Metric Development", BCP 170, RFC 6390,

October 2011.

Authors' Addresses

Claire Bi
Shanghai Research Institure of China Telecom Corporation Limited
No.1835, South Pudong Road
Shanghai 200122
China

EMail: bijy@sttri.com.cn

Alan Clark
Telchemy Incorporated
2905 Premiere Parkway, Suite 280
Duluth, GA 30097
USA

EMail: alan.d.clark@telchemy.com

Geoff Hunt
Unaffiliated

EMail: r.geoff.hunt@gmail.com

Qin Wu
Huawei
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012
China

EMail: sunseawq@huawei.com

Glen Zorn (editor)
Network Zen
227/358 Thanon Sanphawut
Bang Na, Bangkok 10260
Thailand

Phone: +66 (0) 90 920 1060
EMail: glenzorn@gmail.com