XRBLOCK
INTERNET-DRAFT
Intended Status: Standards Track
Expires: July 12, 2015

R. Huang
Huawei
A. Clark
Telchemy

January 8, 2015

RTCP XR Report Block for Loss Concealment Metrics Reporting on Video Applications
draft-huang-xrblock-rtcp-xr-video-lc-05

Abstract

This draft defines a new video loss concealment block type to augment those defined in [RFC3611] and [RFC7294] for use in a range of RTP video applications.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Table of Contents

1 Introduction

Multimedia applications often suffer from packet losses in IP networks. In order to get a reasonable degree of quality in case of packet losses, it is necessary to have loss concealment mechanisms at the decoder. Video loss concealment is a range of techniques to mask the effects of packet loss in video communications.

In some applications, reporting the information of receivers applying video loss concealment could give monitors or senders useful information on application QoE. One example is no-reference video quality evaluation. Video probes located upstream from the video endpoint or terminal may not see loss occurring between the probe and the endpoint, and may also not be fully aware of the specific loss concealment methods being dynamically applied by the video endpoint. Evaluating error concealment is important in the circumstance in estimating the subjective impact of impairments.

This draft defines one new video loss concealment block type to augment those defined in [RFC3611] and [RFC7294] for use in a range of RTP video applications. The metrics defined in this draft belong to the class of transport-related terminal metrics defined in [RFC6792].

1.1 RTCP and RTCP XR Reports

The use of RTCP for reporting is defined in [RFC3550]. [RFC3611] defines an extensible structure for reporting using an RTCP Extended Report (XR). This draft defines a new Extended Report block that MUST be used as defined in [RFC3550] and [RFC3611].

1.2 Performance Metrics Framework

The Performance Metrics Framework [RFC6390] provides guidance on the definition and specification of performance metrics. The RTP Monitoring Architectures [RFC6792] provides guidelines for reporting block format using RTCP XR. The XR block type described in this document are in accordance with the guidelines in [RFC6390] and [RFC6792].

1.3 Applicability

These metrics are applicable to video applications of RTP and the video component of Audio/Video applications in which packet loss concealment mechanisms are incorporated into the receiving endpoint to mitigate the impact of network impairments on QoE. For example, in an IPTV system Set Top Boxes could use this RTCP XR block to report loss and loss concealment metrics to an IPTV management system to

enable the service provider to monitor the quality of the IPTV service being delivered to end users.

2 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 [KEYWORDS].

3 Video Loss Concealment Methods

Video loss concealment mechanisms can be classified into 4 types as follow:

a) Frame freeze

The impaired video frame is not displayed, instead, the previously displayed frame is frozen for the duration of the loss event.

b) Inter-frame extrapolation

If an area of the video frame is damaged by loss, the same area from the previous frame(s) can be used to estimate what the missing pixels would have been. This can work well in a scene with no motion but can be very noticeable if there is significant movement from one frame to another. Simple decoders may simply re-use the pixels that were in the missing area while more complex decoders may try to use several frames to do a more complex extrapolation.

c) Interpolation

A decoder may user the undamaged pixels in the video frame to estimate what the missing block of pixels should have.

d) Error Resilient Encoding

The sender may encode the message in a redundant way so that receiver can correct errors using the redundant information. The redundant data useful for error resiliency performed at the decoder can be embedded into the compressed image/video bitstream. For example, the encoder may select an important area of an original video frame, extract some important characteristics of this area, e.g., motion vector of each macroblock, and imperceptibly embed them into other parts of the video frame. FEC is also another error resilient method.

In this document, we differentiate between frame freeze and the other 3 concealment mechanisms described.

4. Video Loss Concealment Report Block

This block reports the video loss concealment metrics to complement the audio metrics defined in [i.d-ietf-xrblock-rtcp-xr-loss-concealment]. This block may be stacked with other RTCP packets to form compound RTCP packets and share the average reporting interval calculated by the RTCP method described in [RFC3550]. It should be noted that the metrics in this report block are based on measurements that are typically made at the time that a video frame is decoded and rendered for playout. The metrics in this block MUST be measured at a consistent point.

The video loss concealment report block has the following format:

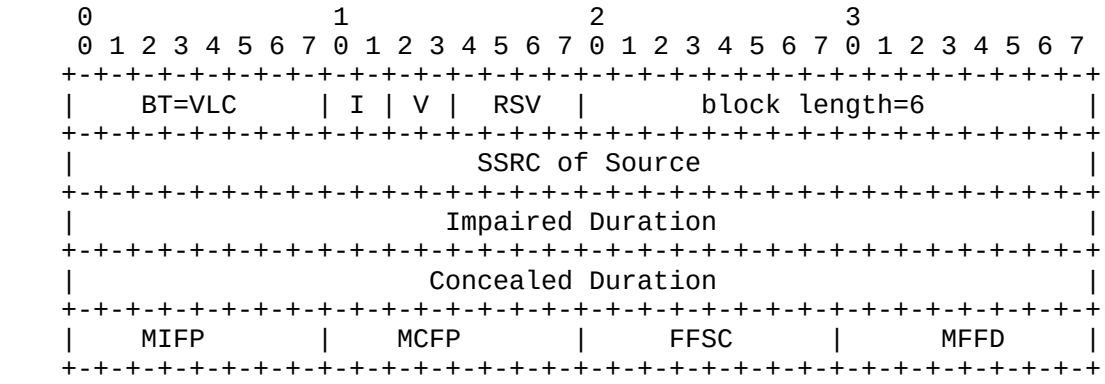

Figure 1: Format for the Video Loss Concealment Report Block

Block Type (BT): 8 bits

A Video Loss Concealment Report Block is identified by the constant VLC.

[Note to RFC Editor: Please replace VLC with the IANA provided RTCP XR block type for this block.]

Interval Metric Flag (I): 2 bits

This field indicates whether the reported metric is an interval, cumulative, or sampled metric [RFC6792]:

I=10: Interval Duration - the reported value applies to the most recent measurement interval duration between successive metrics reports.

I=11: Cumulative Duration - the reported value applies to the

accumulation period characteristic of cumulative measurements.

I=01: Sampled Value - this value MUST NOT be used for this block type.

I=00: Reserved.

Video Loss Concealment Method Type (V): 2 bits

This field is used to identify the video loss concealment method type used at the receiver. Each bit indicates one method type, as follow:

V=10 - Frame freeze
V=11 - Other Loss Concealment Method
V=01&00 - Reserved

block length: 16 bits

This field is in accordance with the definition in [RFC3611]. In this report block, it MUST be set to 6. The block MUST be discarded if the block length is set to a different value.

SSRC of source: 32 bits

As defined in Section 4.1 of [RFC3611].

Impaired Duration: 32 bits

The total time length, expressed in units of RTP timestamp, of video impaired by transmission loss before applying any loss concealment methods.

Two values are reserved: A value of 0xFFFFFFFE indicates out of range (that is, a measured value exceeding 0xFFFFFFFD) and a value of 0xFFFFFFFF indicates that the measurement is unavailable.

Concealed Duration: 32 bits

The total time length, expressed in units of RTP timestamp, of concealed damaged video pictures on which loss concealment method corresponding to V is applied.

Two values are reserved: A value of 0xFFFFFFFE indicates out of range (that is, a measured value exceeding 0xFFFFFFFD) and a value of 0xFFFFFFFF indicates that the measurement is unavailable.

Mean Impaired Frame Proportion (MIFP): 8 bits

Mean Impaired Frame Proportion is the mean proportion of each video frame impaired by loss before applying any loss concealment method during the interval, expressed as a fixed point number with the binary point at the left edge of the field. It is equivalent to taking the integer part after multiplying the loss fraction by 256. If a video frame is totally lost, a value of 0xFF shall be used for the frame when calculating the mean value.

Mean Concealed Frame Proportion (MCFP): 8 bits

Mean Concealed Frame Proportion is the mean proportion of each video frame to which loss concealment (using V) was applied during the interval, expressed as a fixed point number with the binary point at the left edge of the field. It is equivalent to taking the integer part after multiplying the loss fraction by 256. If a lost video frame is totally concealed, a value of 0xFF and if there are no concealed macroblocks, a value of 0, shall be used for the frame when calculating the mean value.

Fraction of Frames Subject to Concealment (FFSC): 8 bits

Fraction of Frames Subject to Concealment is calculated by dividing the number of frames to which loss concealment (using V) was applied by the total number of frames and expressing this value as a fixed point number with the binary point at the left edge of the field. It is equivalent to taking the integer part after multiplying the loss fraction by 256. A value of 0 indicates that there were no concealed frame and a value of 0xFF indicates that the frames in the entire measurement interval are all concealed.

Mean Frame Freeze Duration (MFFD): 8 bits

Mean Frame Freeze Duration is the mean duration of the frame freeze events. The value of MFFD shall be calculated by summing the total duration of all frame freeze events and dividing by the number of events. A value of 0xFF shall be used to indicate a value in excess of 12700 milliseconds. A value of 0 MUST be set when V=11.

5 SDP Signaling

[RFC3611] defines the use of SDP (Session Description Protocol) for signaling the use of RTCP XR blocks. However XR blocks MAY be used without prior signaling (see section 5 of [RFC3611]).

5.1 SDP rtcp-xr-attrib Attribute Extension

This session augments the SDP attribute "rtcp-xr" defined in Section 5.1 of [RFC3611] by providing an additional value of "xr-format" to signal the use of the report block defined in this document.

```
xr-format =/ xr-vlc-block

xr-vlc-block = "video-loss-concealment"
```

5.2 Offer/Answer Usage

When SDP is used in offer-answer context, the SDP Offer/Answer usage defined in [RFC3611] for unilateral "rtcp-xr" attribute parameters applies. For detailed usage of Offer/Answer for unilateral parameter, refer to section 5.2 of [RFC3611].

6 Security Considerations

It is believed that this RTCP XR block introduces no new security considerations beyond those described in [RFC3611]. This block does not provide per-packet statistics, so the risk to confidentially documented in Section 7, paragraph 3 of [RFC3611] does not apply.

An attacker may put incorrect information in the Video Loss Concealment reports, which will be affect the estimation of video loss concealment mechanisms performance and QoE of users. Implementers should consider the guidance in [RFC7202] for using appropriate security mechanisms, i.e., where security is a concern, the implementation should apply encryption and authentication to the report block. For example, this can be achieved by using the AVPF profile together with the Secure RTP profile as defined in [RFC3711]; an appropriate combination of the two profiles (an "SAVPF") is specified in [RFC5124]. However, other mechanisms also exist (documented in [RFC7201]) and might be more suitable.

7 IANA Considerations

New block types for RTCP XR are subject to IANA registration. For general guidelines on IANA considerations for RTCP XR, refer to [RFC3611].

7.1 New RTCP XR Block Type Value

This document assigns the block type value VLC in the IANA "RTP Control Protocol Extended Reports (RTCP XR) Block Type Registry" to the "Video Loss Concealment Metrics Report Block".

[Note to RFC Editor: please replace VLC with the IANA provided RTCP XR block type for this block.]

7.2 New RTCP XR SDP Parameter

This document also registers a new parameter "video-loss-concealment" in the "RTP Control Protocol Extended Reports (RTCP XR) Session Description Protocol (SDP) Parameters Registry".

7.3 Contact Information for registrations

The following contact information is provided for all registrations in this document:

Rachel Huang (rachel.huang@huawei.com)

101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012
China

8 Acknowledgements

The author would like to thank Colin Perkins, Roni Even for their valuable comments.

9 References

9.1 Normative References

[KEYWORDS] 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., Ed., Caceres, R., Ed., and A. Clark, Ed., "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.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

[RFC5124] Ott, J. and E. Carrara, "Extended Secure RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/SAVPF)", RFC 5124, February 2008.

[RFC5105] Lendl, O., "ENUM Validation Token Format Definition", RFC 5105, December 2007.

[RFC4588] Rey, J., Leon, D., Miyazaki, A., Varsa, V., and R. Hakenberg, "RTP Retransmission Payload Format", RFC 4588, July 2006.

[RFC7201] Westerlund, M. and C., Perkins, "Qptions for Securing RTP Sessions", RFC 7201, April 2014.

[RFC7202] Perkins, C. and M., Westerlund, "Securing the RTP Framework: Why RTP Does Not Mandate a Single Media Security Solution", RFC 7202, April 2014.

[RFC7294] Clark, A., Zorn, G., Bi, C. and Q., Wu, "RTCP XR Report Block for Concealment Metrics Reporting on Audio Applications", April 2014.

9.2 Informative References

[RFC6390] Clark, A. and B. Claise, "Guidelines for Considering New Performance Metric Development", BCP 170, RFC 6390, October 2011.

[RFC6792] Wu, Q., Hunt, G., and P. Arden, "Guidelines for Use of the RTP Monitoring Framework", RFC 6792, November 2012.

Appendix A. Metrics Represented Using the Template from RFC 6390

TBD.

Authors' Addresses

Rachel Huang
Huawei
101 Software Avenue, Yuhua District
Nanjing 210012
China

EMail: rachel.huang@huawei.com

Alan Clark
Telchemy Incorporated
2905 Premiere Parkway, Suite 280

Duluth, GA 30097
USA

Email: alan.d.clark@telchemy.com

XR Block Working Group
Internet-Draft
Intended status: Informational
Expires: November 26, 2018

V. Singh
callstats.io
R. Huang
R. Even
Huawei
D. Romascanu
Individual
L. Deng
China Mobile

May 25, 2018

Considerations for Selecting RTCP Extended Report (XR) Metrics for the WebRTC Statistics API
draft-ietf-xrblock-rtcweb-rtcp-xr-metrics-10

Abstract

This document describes monitoring features related to media streams in Web real-time communication (WebRTC). It provides a list of RTCP Sender Report, Receiver Report and Extended Report metrics, which may need to be supported by RTP implementations in some diverse environments. It lists a set of identifiers for the WebRTC's statistics API. These identifiers are a set of RTCP SR, RR, and XR metrics related to the transport of multimedia flows.

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 21, 2018.

Copyright Notice

Table of Contents

1. Introduction

Web real-time communication (WebRTC) [I-D.ietf-rtcweb-overview] deployments are emerging and applications need to be able to estimate the service quality. If sufficient information (metrics or statistics) is provided to the application, it can attempt to improve the media quality. [RFC7478] specifies a requirement for statistics:

F38 The browser must be able to collect statistics, related to the transport of audio and video between peers, needed to estimate quality of experience.

The WebRTC Stats API [W3C.WD-webrtc-stats] currently lists metrics reported in the RTCP Sender and Receiver Report (SR/RR) [RFC3550] to fulfill this requirement. However, the basic metrics from RTCP SR/RR are not sufficient for precise quality monitoring, or diagnosing potential issues.

Standards such as "RTP Control Protocol Extended Reports (RTCP XR)" [RFC3611] as well as other extensions standardized in the XRBLOCK working group, e.g., burst/gap loss metric reporting [RFC6958], burst/gap discard metric reporting [RFC7003], and etc., have been produced for the purpose of collecting and reporting performance metrics from RTP endpoint devices that can be used to have a end-to-end service visibility and measure the delivering quality in various RTP services. These metrics are able to complement those in [RFC3550].

In this document, we provide rationale for choosing additional RTP metrics for the WebRTC getStats() API [W3C.WD-webrtc]. All identifiers proposed in this document are recommended to be implemented by an WebRTC endpoint. An endpoint may choose not to expose an identifier if it does not implement the corresponding RTCP Report. This document only considers RTP layer metrics. Other metrics, e.g., IP layer metrics, are out of scope.

2. Terminology

ReportGroup: It is a set of metrics identified by a common Synchronization source (SSRC).

3. RTP Statistics in WebRTC Implementations

The RTCP Sender Reports (SRs) and Receiver Reports (RRs) [RFC3550] expose the basic metrics for the local and remote media streams. However, these metrics provide only partial or limited information, which may not be sufficient for diagnosing problems or quality monitoring. For example, it may be useful to distinguish between packets lost and packets discarded due to late arrival. Even though they have the same impact on the multimedia quality, it helps in identifying and diagnosing problems. RTP Control Protocol Extended Reports (XRs) [RFC3611] and other extensions discussed in the XRBLOCK working group provide more detailed statistics, which complement the basic metrics reported in the RTCP SR and RRs.

The WebRTC application extracts the statistic from the browser by querying the getStats() API [W3C.WD-webrtc]. The browser can easily report the local variables i.e., the statistics related to the outgoing RTP media streams and the incoming RTP media streams. However, without the support of RTCP XRs or some other signaling mechanism, the WebRTC application cannot expose the remote endpoints' statistics. [I-D.ietf-rtcweb-rtp-usage] does not mandate the use of any RTCP XRs and their usage is optional. If the use of RTCP XRs is successfully negotiated between endpoints (via SDP), thereafter the application has access to both local and remote statistics. Alternatively, once the WebRTC application gets the local information, they can report it to an application server or a third-party monitoring system, which provides quality estimations or diagnosis services for application developers. The exchange of statistics between endpoints or between a monitoring server and an endpoint is outside the scope of this document.

4. Considerations for Impact of Measurement Interval

RTCP extensions like RTCP XR usually share the same timing interval with the RTCP SR/RR, i.e., they are sent as compound packets, together with the RTCP SR/RR. Alternatively, if the RTCP XR uses a different measurement interval, all XRs using the same measurement interval are compounded together and the measurement interval is indicated in a specific measurement information block defined in [RFC6776].

When using WebRTC getStats() APIs (see section 7 of [W3C.WD-webrtc]), the applications can query this information at arbitrary intervals. For the statistics reported by the remote endpoint, e.g., those conveyed in an RTCP SR/RR/XR, these will not change until the next RTCP report is received. However, statistics generated by the local endpoint have no such restrictions as long as the endpoint is sending and receiving media. For example, an application may choose to poll

the stack for statistics every 1 second. In this case the underlying stack local will return the current snapshot of the local statistics (for incoming and outgoing media streams). However, it may return the same remote statistics as before for the remote statistics, as no new RTCP reports may have been received in the past 1 second. This can occur when the polling interval is shorter than the average RTCP reporting interval.

5. Candidate Metrics

Since the following metrics are all defined in RTCP XR, which is not mandated in WebRTC, all of them are local. However, if RTCP XR is supported by negotiation between two browsers, the following metrics can also be generated remotely and be sent to local by RTCP XR packets.

The following metrics are classified into 3 categories: network impact metrics, application impact metrics and recovery metrics. Network impact metrics are the statistics recording the information only for network transmission. They are useful for network problem diagnosis. Application impact metrics mainly collect the information from the viewpoint of application, e.g., bit rate, frame rate or jitter buffers. Recovery metrics reflect how well the repair mechanisms perform, e.g. loss concealment, retransmission or Forward Error Correction (FEC). All of the 3 types of metrics are useful for quality estimations of services in WebRTC implementations. WebRTC applications can use these metrics to calculate the estimated Mean Opinion Score (MOS) [ITU-T P.800.1] values or Media Delivery Index (MDI) [RFC4445] for their services.

5.1. Network Impact Metrics

5.1.1. Loss and Discard Packet Count Metric

In multimedia transport, packets which are received abnormally are classified into 3 types: lost, discarded and duplicate packets. Packet loss may be caused by network device breakdown, bit-error corruption or network congestion (packets dropped by an intermediate router queue). Duplicate packets may be a result of network delays that causes the sender to retransmit the original packets. Discarded packets are packets that have been delayed long enough (perhaps they missed the playout time) and are considered useless by the receiver. Lost and discarded packets cause problems for multimedia services, as missing data and long delays can cause degradation in service quality, e.g., missing large blocks of contiguous packets (lost or discarded) may cause choppy audio, and long network transmission delay time may cause audio or video buffering. The RTCP SR/RR defines a metric for counting the total number of RTP data packets

that have been lost since the beginning of reception. But this statistic does not distinguish lost packets from discarded and duplicate packets. Packets that arrive late will be discarded and are not reported as lost, and duplicate packets will be regarded as a normally received packet. Hence, the loss metric can be misleading if many duplicate packets are received or packets are discarded, which causes the quality of the media transport to appear okay from the statistic point of view, but meanwhile the users may actually be experiencing bad service quality. So in such cases, it is better to use more accurate metrics in addition to those defined in RTCP SR/RR.

The lost packets and duplicated packets metrics defined in Statistics Summary Report Block of [RFC3611] extend the information of loss carried in standard RTCP SR/RR. They explicitly give an account of lost and duplicated packets. Lost packet counts are useful for network problem diagnosis. It is better to use the loss packets metrics of [RFC3611] to indicate the packet lost count instead of the cumulative number of packets lost metric of [RFC3550]. Duplicated packets are usually rare and have little effect on QoS evaluation. So it may not be suitable for use in WebRTC.

Using loss metrics without considering discard metrics may result in inaccurate quality evaluation, as packet discard due to jitter is often more prevalent than packet loss in modern IP networks. The discarded metric specified in [RFC7002] counts the number of packets discarded due to the jitter. It augments the loss statistics metrics specified in standard RTCP SR/RR. For those RTCWEB services with jitter buffers requiring precise quality evaluation and accurate troubleshooting, this metric is useful as a complement to the metrics of RTCP SR/RR.

5.1.2. Burst/Gap Pattern Metrics for Loss and Discard

RTCP SR/RR defines coarse metrics regarding loss statistics: the metrics are all about per call statistics and are not detailed enough to capture the transitory nature of some impairments like bursty packet loss. Even if the average packet loss rate is low, the lost packets may occur during short dense periods, resulting in short periods of degraded quality. Bursts cause lower quality experience than the non-bursts for low packet loss rates, whereas for high packet loss rates the converse is true. So capturing burst gap information is very helpful for quality evaluation and locating impairments. If the WebRTC application needs to evaluate the services quality, burst gap metrics provides more accurate information than RTCP SR/RR.

[RFC3611] introduces burst gap metrics in VoIP report block. These metrics record the density and duration of burst and gap periods,

which are helpful in isolating network problems since bursts correspond to periods of time during which the packet loss/discard rate is high enough to produce noticeable degradation in audio or video quality. Burst gap related metrics are also introduced in [RFC7003] and [RFC6958] which define two new report blocks for usage in a range of RTP applications beyond those described in [RFC3611]. These metrics distinguish discarded packets from loss packets that occur in the bursts period and provides more information for diagnosing network problems. Additionally, the block reports the frequency of burst events which is useful information for evaluating the quality of experience. Hence, if WebRTC applications need to do quality evaluation and observe when and why quality degrades, these metrics should be considered.

5.1.3. Run Length Encoded Metrics for Loss, Discard

Run-length encoding uses a bit vector to encode information about the packet. Each bit in the vector represents a packet and depending on the signaled metric it defines if the packet was lost, duplicated, discarded, or repaired. An endpoint typically uses the run length encoding to accurately communicate the status of each packet in the interval to the other endpoint. [RFC3611], [RFC7097] define run-length encoding for lost and duplicate packets, and discarded packets, respectively.

The WebRTC application could benefit from the additional information. If losses occur after discards, an endpoint may be able to correlate the two run length vectors to identify congestion-related losses, e.g., a router queue became overloaded causing delays and then overflowed. If the losses are independent, it may indicate bit-error corruption. For the WebRTC Stats API [W3C.WD-webrtc-stats], these types of metrics are not recommended for use due to the large amount of data and the computation involved.

5.2. Application Impact Metrics

5.2.1. Discarded Octets Metric

The metric reports the cumulative size of the packets discarded in the interval. It is complementary to number of discarded packets. An application measures sent octets and received octets to calculate sending rate and receiving rate, respectively. The application can calculate the actual bit rate in a particular interval by subtracting the discarded octets from the received octets.

For WebRTC, discarded octets supplements the sent and received octets and provides an accurate method for calculating the actual bit rate which is an important parameter to reflect the quality of the media.

The discarded bytes metric is defined in [RFC7243].

5.2.2. Frame Impairment Summary Metrics

RTP has different framing mechanisms for different payload types. For audio streams, a single RTP packet may contain one or multiple audio frames. On the other hand, in video streams, a single video frame may be transmitted in multiple RTP packets. The size of each packet is limited by the Maximum Transmission Unit (MTU) of the underlying network. However, statistics from standard SR/RR only collect information from transport layer, which may not fully reflect the quality observed by the application. Video is typically encoded using two frame types i.e., key frames and derived frames. Key frames are normally just spatially compressed, i.e., without prediction from other pictures. The derived frames are temporally compressed, i.e., depend on the key frame for decoding. Hence, key frames are much larger in size than derived frames. The loss of these key frames results in a substantial reduction in video quality. Thus it is reasonable to consider this application layer information in WebRTC implementations, which influence sender strategies to mitigate the problem or require the accurate assessment of users' quality of experience.

The metrics in this category include: number of discarded key frames, number of lost key frames, number of discarded derived frames, number of lost derived frames. These metrics can be used to calculate Media Loss Rate (MLR) of MDI [RFC4445]. Details of the definition of these metrics are described in [RFC7003]. Additionally, the metric provides the rendered frame rate, an important parameter for quality estimation.

5.2.3. Jitter Buffer Metrics

The size of the jitter buffer affects the end-to-end delay on the network and also the packet discard rate. When the buffer size is too small, slower packets are not played out and dropped, while when the buffer size is too large, packets are held longer than necessary and consequently reduce conversational quality. Measurement of jitter buffer should not be ignored in the evaluation of end user perception of conversational quality. Jitter buffer related metrics, such as maximum and nominal jitter buffer, could be used to show how the jitter buffer behaves at the receiving endpoint. They are useful for providing better end-user quality of experience (QoE) when jitter buffer factors are used as inputs to calculate estimated MOS values. Thus for those cases, jitter buffer metrics should be considered. The definition of these metrics is provided in [RFC7005].

5.3. Recovery metrics

This document does not consider concealment metrics [RFC7294] as part of recovery metrics.

5.3.1. Post-repair Packet Count Metrics

Web applications can support certain RTP error-resilience mechanisms following the recommendations specified in [draft-ietf-rtcweb-rtp-usage]. For these web applications using repair mechanisms, providing some statistic information for the performance of their repair mechanisms could help to have a more accurate quality evaluation.

The unrepaired packet count and repaired loss count defined in [RFC7509] provide the recovery information of the error-resilience mechanisms to the monitoring application or the sending endpoint. The endpoint can use these metrics to ascertain the ratio of repaired packets to lost packets. Including post-repair packet count metrics helps the application evaluate the effectiveness of the applied repair mechanisms.

5.3.2. Run Length Encoded Metric for Post-repair

[RFC5725] defines run-length encoding for post-repair packets. When using error-resilience mechanisms, the endpoint can correlate the loss run length with this metric to ascertain where the losses and repairs occurred in the interval. This provides more accurate information for recovery mechanisms evaluation than those in Section 5.3.1. However, it is not suggested to use due to their enormous amount of data when RTCP XR are supported.

For WebRTC, the application may benefit from the additional information. If losses occur after discards, an endpoint may be able to correlate the two run length vectors to identify congestion-related losses, e.g., a router queue became overloaded causing delays and then overflowed. If the losses are independent, it may indicate bit-error corruption. Lastly, when using error-resilience mechanisms, the endpoint can correlate the loss and post-repair run lengths to ascertain where the losses and repairs occurred in the interval. For example, consecutive losses are likely not to be repaired by a simple FEC scheme.

6. Identifiers from Sender, Receiver, and Extended Report Blocks

This document describes a list of metrics and corresponding identifiers relevant to RTP media in WebRTC. This group of identifiers are defined on a ReportGroup corresponding to a synchronization source (SSRC). In practice the application needs to be able to query the statistic identifiers on both an incoming (remote) and outgoing (local) media stream. Since sending and

receiving SR and RR are mandatory, the metrics defined in the SR and RR report blocks are always available. For XR metrics, it depends on two factors: 1) if it is measured at the endpoint, 2) if it is reported by the endpoint in an XR report. If a metric is only measured by the endpoint and not reported, the metrics will only be available for the incoming (remote) media stream. Alternatively, if the corresponding metric is also reported in an XR report, it will be available for both the incoming (remote) and outgoing (local) media stream.

For a remote statistic, the timestamp represents the timestamp from an incoming SR/RR/XR packet. Conversely, for a local statistic, it refers to the current timestamp generated by the local clock (typically the POSIX timestamp, i.e., milliseconds since Jan 1, 1970).

As per [RFC3550], the octets metrics represent the payload size (i.e., not including header or padding).

6.1. Cumulative Number of Packets and Octets Sent

Name: packetsSent

Definition: section 6.4.1 in [RFC3550].

Name: bytesSent

Definition: section 6.4.1 in [RFC3550].

6.2. Cumulative Number of Packets and Octets Received

Name: packetsReceived

Definition: section 6.4.1 in [RFC3550].

Name: bytesReceived

Definition: section 6.4.1 in [RFC3550].

6.3. Cumulative Number of Packets Lost

Name: packetsLost

Definition: section 6.4.1 in [RFC3550].

6.4. Interval Packet Loss and Jitter

Name: jitter

Definition: section 6.4.1 in [RFC3550].

Name: fractionLost

Definition: section 6.4.1 in [RFC3550].

6.5. Cumulative Number of Packets and Octets Discarded

Name: packetsDiscarded

Definition: The cumulative number of RTP packets discarded due to late or early-arrival, Appendix A (a) of [RFC7002].

Name: bytesDiscarded

Definition: The cumulative number of octets discarded due to late or early-arrival, Appendix A of [RFC7243].

6.6. Cumulative Number of Packets Repaired

Name: packetsRepaired

Definition: The cumulative number of lost RTP packets repaired after applying a error-resilience mechanism, Appendix A (b) of [RFC7509]. To clarify, the value is upper bound to the cumulative number of lost packets.

6.7. Burst Packet Loss and Burst Discards

Name: burstPacketsLost

Definition: The cumulative number of RTP packets lost during loss bursts, Appendix A (c) of [RFC6958].

Name: burstLossCount

Definition: The cumulative number of bursts of lost RTP packets, Appendix A (e) of [RFC6958].

Name: burstPacketsDiscarded

Definition: The cumulative number of RTP packets discarded during discard bursts, Appendix A (b) of [RFC7003].

Name: burstDiscardCount

Definition: The cumulative number of bursts of discarded RTP packets, Appendix A (e) of [RFC8015].

[RFC3611] recommends a Gmin (threshold) value of 16 for classifying packet loss or discard burst.

6.8. Burst/Gap Rates

Name: burstLossRate

Definition: The fraction of RTP packets lost during bursts, Appendix A (a) of [RFC7004].

Name: gapLossRate

Definition: The fraction of RTP packets lost during gaps, Appendix A (b) of [RFC7004].

Name: burstDiscardRate

Definition: The fraction of RTP packets discarded during bursts, Appendix A (e) of [RFC7004].

Name: gapDiscardRate

Definition: The fraction of RTP packets discarded during gaps, Appendix A (f) of [RFC7004].

6.9. Frame Impairment Metrics

Name: framesLost

Definition: The cumulative number of full frames lost, Appendix A (i) of [RFC7004].

Name: framesCorrupted

Definition: The cumulative number of frames partially lost, Appendix A (j) of [RFC7004].

Name: framesDropped

Definition: The cumulative number of full frames discarded, Appendix A (g) of [RFC7004].

Name: framesSent

Definition: The cumulative number of frames sent.

Name: framesReceived

Definition: The cumulative number of partial or full frames received.

7. Adding new metrics to WebRTC Statistics API

During the progress of this work, the metrics defined in this draft have already been added to the W3C WebRTC specification. The working process to add new metrics for future is to create an issue or pull request on the repository of the W3C WebRTC specification (https://github.com/w3c/webrtc-stats).

8. Security Considerations

This document focuses on listing the RTCP XR metrics defined in the corresponding RTCP reporting extensions and do not give rise to any new security vulnerabilities beyond those described in [RFC3611] and [RFC6792].

The overall security considerations for RTP used in WebRTC applications is described in [I-D.ietf-rtcweb-rtp-usage] and [I-D.ietf-rtcweb-security], which are also apply to this memo.

9. IANA Consideration

This document requests no action by IANA.

10. Acknowledgements

The authors would like to thank Bernard Aboba, Harald Alvestrand, Al Morton, Colin Perkins, and Shida Schubert for their valuable comments and suggestions on earlier version of this document.

11. References

11.1. Normative References

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, DOI 10.17487/RFC3550, July 2003, <http://www.rfc-editor.org/info/rfc3550>.

[RFC3611] Friedman, T., Ed., Caceres, R., Ed., and A. Clark, Ed., "RTP Control Protocol Extended Reports (RTCP XR)", RFC 3611, DOI 10.17487/RFC3611, November 2003, <http://www.rfc-editor.org/info/rfc3611>.

[RFC5725] Begen, A., Hsu, D., and M. Lague, "Post-Repair Loss RLE Report Block Type for RTP Control Protocol (RTCP) Extended Reports (XRs)", RFC 5725, DOI 10.17487/RFC5725, February 2010, <http://www.rfc-editor.org/info/rfc5725>.

[RFC6776] Clark, A. and Q. Wu, "Measurement Identity and Information Reporting Using a Source Description (SDES) Item and an RTCP Extended Report (XR) Block", RFC 6776, DOI 10.17487/RFC6776, October 2012, <http://www.rfc-editor.org/info/rfc6776>.

[RFC6792] Qu, Q. and P. Arden, "Guidelines for Use of the RTP Monitoring Framework", RFC 6792, November 2012, <http://www.rfc-editor.org/info/rfc6792>

[RFC6958] Clark, A., Zhang, S., Zhao, J., and Q. Wu, Ed., "RTP Control Protocol (RTCP) Extended Report (XR) Block for Burst/Gap Loss Metric Reporting", RFC 6958, DOI 10.17487/RFC6958, May 2013, <http://www.rfc-editor.org/info/rfc6958>.

[RFC7002] Clark, A., Zorn, G., and Q. Wu, "RTP Control Protocol (RTCP) Extended Report (XR) Block for Discard Count Metric Reporting", RFC 7002, DOI 10.17487/RFC7002, September 2013, <http://www.rfc-editor.org/info/rfc7002>.

[RFC7003] Clark, A., Huang, R., and Q. Wu, Ed., "RTP Control Protocol (RTCP) Extended Report (XR) Block for Burst/Gap Discard Metric Reporting", RFC 7003, DOI 10.17487/RFC7003, September 2013, <http://www.rfc-editor.org/info/rfc7003>.

[RFC7004] Zorn, G., Schott, R., Wu, Q., Ed., and R. Huang, "RTP Control Protocol (RTCP) Extended Report (XR) Blocks for Summary Statistics Metrics Reporting", RFC 7004, DOI 10.17487/RFC7004, September 2013, <http://www.rfc-editor.org/info/rfc7004>.

[RFC7005] Clark, A., Singh, V., and Q. Wu, "RTP Control Protocol (RTCP) Extended Report (XR) Block for De-Jitter Buffer Metric Reporting", RFC 7005, DOI 10.17487/RFC7005, September 2013, <http://www.rfc-editor.org/info/rfc7005>.

[RFC7097] Ott, J., Singh, V., Ed., and I. Curcio, "RTP Control Protocol (RTCP) Extended Report (XR) for RLE of Discarded

Packets", RFC 7097, DOI 10.17487/RFC7097, January 2014, <http://www.rfc-editor.org/info/rfc7097>.

[RFC7243] Singh, V., Ed., Ott, J., and I. Curcio, "RTP Control Protocol (RTCP) Extended Report (XR) Block for the Bytes Discarded Metric", RFC 7243, DOI 10.17487/RFC7243, May 2014, <http://www.rfc-editor.org/info/rfc7243>.

[RFC7509] Huang, R. and V. Singh, "RTP Control Protocol (RTCP) Extended Report (XR) for Post-Repair Loss Count Metrics", RFC 7509, DOI 10.17487/RFC7509, May 2015, <http://www.rfc-editor.org/info/rfc7509>.

[RFC8015] Singh, V., Perkins, C., Clark, A., and R. Huang, "RTP Control Protocol (RTCP) Extended Report (XR) Block for Independent Reporting of Burst/Gap Discard Metrics", RFC 8015, DOI 10.17487/RFC8015, November 2016, <http://www.rfc-editor.org/info/rfc8015>.

11.2. Informative References

[I-D.ietf-rtcweb-overview] H. Alverstrand, "Overview: Real Time Protocols for Browser-based Applications", draft-ietf-rtcweb-overview-19 (work in progress), November 2017.

[ITU-T P.800.1] "Mean Opinion Score (MOS) terminology", ITU-T P.800.1, July 2016.

[RFC4445] Welch, J. and J. Clark, "A Proposed Media Delivery Index (MDI)", RFC4445, April 2006.

[I-D.ietf-rtcweb-rtp-usage] Perkins, C., Westerlund, M., and J. Ott, "Web Real-Time Communication (WebRTC): Media Transport and Use of RTP", draft-ietf-rtcweb-rtp-usage-26 (work in progress), March 2016.

[I-D.ietf-rtcweb-security] Rescorla, E., "Security Considerations for WebRTC", draft-ietf-rtcweb-security-10 (work in progress), January 2018.

[RFC7294] Clark, A., Zorn, G., Bi, C. and Q. Wu, "RTP Control Protocol (RTCP) Extended Report (XR) Blocks for Concealment Metrics Reporting on Audio Applications", RFC 7294, July 2014, <http://www.rfc-editor.org/info/rfc7294>

[RFC7478] Holmberg, C., Hakansson, S., and G. Eriksson, "Web Real-Time Communication Use Cases and Requirements", RFC 7478,

DOI 10.17487/RFC7478, March 2015, <http://www.rfc-editor.org/info/rfc7478>.

[W3C.WD-webrtc] Bergkvist, A., Burnett, C., Jennings, C., Narayanan, A., Aboba B. and T. Brandstetter, "WebRTC 1.0: Real-time Communication Between Browsers", World Wide Web Consortium WD WD-webrtc-20171102, November 2017, <https://www.w3.org/TR/2017/CR-webrtc-20171102/>.

[W3C.WD-webrtc-stats] Alvestrand, H. and V. Singh, "Identifiers for WebRTC's Statistics API", World Wide Web Consortium WD WD-webrtc-stats-20180519, May 2018, <https://www.w3.org/TR/2018/WD-webrtc-stats-20180519/>.

Authors' Addresses

Varun Singh
CALLSTATS I/O Oy
Annankatu 31-33 C 42
Helsinki 00100
Finland

Email: varun@callstats.io
URI: https://www.callstats.io/about

Rachel Huang
Huawei
101 Software Avenue, Yuhua District
Nanjing, CN 210012
China

Email: rachel.huang@huawei.com

Roni Even
Huawei
14 David Hamelech
Tel Aviv 64953
Israel

Email: roni.even@huawei.com

Dan Romascanu

Email: dromasca@gmail.com

Lingli Deng
China Mobile

Email: denglingli@chinamobile.com