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

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

Audio/Video Transport Working Group V. Singh, Ed.
Internet-Draft callstats.io
Intended status: Standards Track C. Perkins
Expires: April 22, 2016 University of Glasgow
A. Clark
Telchemy
R. Huang
Huawei
October 20, 2015

RTP Control Protocol (RTCP) Extended Report (XR) Block for Independent Reporting of Burst/Gap Discard Metric

draft-singh-xrblock-independent-burst-gap-discard-01

Abstract

This document defines an RTP Control Protocol (RTCP) Extended Report (XR) block that allows the reporting of burst and gap discard metrics independently of the burst and gap loss metrics for use in a range of RTP applications.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

1.1. Burst-Gap Discard Metrics Block

This document defines a new block type that extends the metrics defined in [RFC7003], the metrics in this report block can be used in a range of RTP applications. The new block type reports the proportion of packets discarded by the jitter buffer at the receiver in a burst and number of packets discarded depends on the dejitter buffer algorithm implemented by the endpoint.

The new report block defined in this document is different from the one defined in [RFC7003]. The metrics in [RFC7003] depends on the metrics in the burstgap loss metric defined in [RFC6958].

Consequently, an endpoint using [RFC7003] MUST report it along with [RFC6958] for it to be useful. The combined usage is useful when an endpoint observes correlated packet losses and discard. However, when the burst of packet losses and discards do not occur simultaneously, the application may prefer a concise report block that just reports the burstgap of discarded packets. The report block in this document provides the complete information and does not require additional report blocks. That is, this block reports: the total number of packets discarded, the total burst duration, and the total number of bursts, all of these metrics are missing in [RFC7003].

This block provides information on transient network issues. Burst/gap metrics are typically used in cumulative reports; however, they may also be used in interval reports (see the Interval Metric flag in Section 3.2). The variation in the number of packet discard in a burst affects the user experience. Based on the metrics reported in the block, the sending endpoint may change the packetisation interval, vary the bitrate, etc. The report may additionally be used for diagnostics [RFC6792]. The metric belongs to the class of transport-related end-system metrics defined in [RFC6792].

The definitions of "burst", "gap", "loss", and "discard" are consistent with the definitions in [RFC3611]. To accommodate the range of jitter buffer algorithms and packet discard logic that may be used by implementors, the method used to distinguish between bursts and gaps shall use an equivalent method to that defined in Section 4.7.2 of [RFC3611]. Note that reporting the specific jitter buffer algorithms and/or packet discard logic is out of the scope of this document.

1.2. RTCP and RTCP Extended Reports

The use of RTCP for reporting is defined in [RFC3550]. [RFC3611] defined an extensible structure for reporting using an RTCP Extended Report (XR). This document defines a new Extended Report block for use with [RFC3550] and [RFC3611].

1.3. Performance Metrics Framework

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

1.4. Applicability

These metrics are applicable to a range of RTP applications that contain de-jitter buffers [RFC5481] at the receiving end to smooth variation in packet-arrival time and don’t use stream repair means, e.g., Forward Error Correction (FEC) [I-D.ietf-payload-flexible-fec-scheme] and/or retransmission [RFC4588].

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 RFC 2119 [RFC2119].

In addition, the following terms are defined:

Received, Lost, and Discarded

A packet shall be regarded as "lost" if it fails to arrive within an implementation-specific time window. A packet that arrives within this time window but is too early to be played out, too late to be played out, or thrown away before playout due to packet duplication or redundancy shall be regarded as discarded. A packet shall not be regarded as discarded if it arrives within this time window but is dropped during decoding by some higher-layer decoder, e.g., due to a decoding error. A packet shall be classified as one of received (or OK), discarded, or lost. The metric "cumulative number of packets lost" defined in [RFC3550] reports a count of packets lost from the media stream (single synchronization source (SSRC) within a single RTP session). Similarly, the metric "number of packets discarded" defined in [RFC7002] reports a count of packets discarded from the media stream (single SSRC within a single RTP session) arriving at the receiver. Another metric, defined in [RFC5725], is available to report on packets that are not recovered by any repair techniques that may be in use. Note that the term "discard" defined here builds on the "discard" definition in [RFC3611] but extends the concept to take into account packet duplication and reports different types of discard counts [RFC7002].

Bursts and Gaps

The terms "burst" and "gap" are used in a manner consistent with that of RTCP XR [RFC3611]. RTCP XR views an RTP stream as being divided into bursts, which are periods during which the discard rate is high enough to cause noticeable quality degradation (generally over 5 percent discard rate), and gaps, which are periods during which discarded packets are infrequent and hence quality is generally acceptable.

3. Burst/Gap Discard Metrics Block

Metrics in this block report on burst/gap discard in the stream arriving at the RTP system. Measurements of these metrics are made at the receiving end of the RTP stream. Instances of this metrics block use the synchronization source (SSRC) to refer to the separate auxiliary Measurement Information Block [RFC6776], which describes measurement periods in use (see [RFC6776], Section 4.2).

This metrics block relies on the measurement period in the Measurement Information Block indicating the span of the report. Senders MUST send this block in the same compound RTCP packet as the Measurement Information Block. Receivers MUST verify that the measurement period is received in the same compound RTCP packet as this metrics block. If not, this metrics block MUST be discarded.

3.1. Report Block Structure

The structure of the Burst/Gap Discard Metrics Block is as follows.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    BT=IBGD    | I |   resv    |      Block Length = 5         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        SSRC of Source                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Threshold   |         Sum of Burst Durations (ms)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Packets Discarded in Bursts          |    Number of  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Bursts     |           Total Packets Expected in Bursts    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Discard Count                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Report Block Structure

3.2. Definition of Fields in Burst/Gap Discard Metrics Block

Block Type (BT): 8 bits

A Burst/Gap Discard Metrics Block is identified by the constant IBGD.

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

Interval Metric flag (I): 2 bits

This field is used to indicate whether the burst/gap discard metrics are Sampled, Interval, or Cumulative metrics [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 - the reported value is a sampled instantaneous value.

In this document, burst/gap discard metrics can only be measured over definite intervals and cannot be sampled. Also, the value I=00 is reserved for future use. Senders MUST NOT use the values I=00 or I=01. If a block is received with I=00 or I=01, the receiver MUST discard the block.

Reserved (resv): 6 bits

These bits are reserved. They MUST be set to zero by senders and ignored by receivers (see [RFC6709], Section 4.2).

Block Length: 16 bits

The length of this report block in 32-bit words, minus one. For the Burst/Gap Discard Metrics Block, the block length is equal to 5. 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].

Threshold: 8 bits

The Threshold is equivalent to Gmin in [RFC3611], i.e., the number of successive packets that must not be discarded prior to and following a discard packet in order for this discarded packet to be regarded as part of a gap. Note that the Threshold is set in accordance with the Gmin calculation defined in Section 4.7.2 of [RFC3611].

Sum of Burst Durations (ms): 24 bits

The total duration of bursts of discarded packets in the period of the report (Interval or Cumulative).

The measured value is an unsigned value. If the measured value exceeds 0xFFFFFD, the value 0xFFFFFE MUST be reported to indicate an over-range measurement. If the measurement is unavailable, the value 0xFFFFFF MUST be reported.

Packets Discarded in Bursts: 24 bits

The total number of packets discarded during discard bursts, as defined in Section 3.2 of [RFC7002].

Number of Bursts: 16 bits

The number of discard bursts in the period of the report (Interval or Cumulative).

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

Total Packets Expected in Bursts: 24 bits

The total number of packets expected during discarded bursts (that is, the sum of received packets and lost packets). The metric is defined in [RFC7003].

Discard Count: 32 bits

Number of packets discarded over the period (Interval or Cumulative) covered by this report, as defined in Section 3.2 of [RFC7002].

3.3. Derived Metrics Based on the Reported Metrics

The metrics described here are intended to be used in conjunction with information from the Measurement Information Block [RFC6776].

These metrics provide the following information relevant to statistical parameters (depending on cumulative of interval measures), for example:

- o The average discarded burst size, which can be calculated by dividing the metric "Packets Discarded in Bursts" with the "Number of Bursts".

- o The average burst duration, which can be calculated by dividing the metric "Sum of Burst Durations (ms)" with the "Number of bursts".

4. Considerations for Voice-over-IP Applications

This metrics block is applicable to a broad range of RTP applications. Where the metric is used with a Voice-over-IP (VoIP) application and the stream repair means is not available, the following considerations apply.

RTCP XR views a call as being divided into bursts, which are periods during which the discard rate is high enough to cause noticeable call quality degradation (generally over 5 percent discard rate) and gaps, which are periods during which discarded packets are infrequent and hence call quality is generally acceptable.

If voice activity detection is used, the burst and gap duration shall be determined as if silence packets had been sent, i.e., a period of silence in excess of Gmin packets will terminate a burst condition.

The recommended value for the threshold Gmin in [RFC3611] results in a burst being a period of time during which the call quality is degraded to a similar extent to a typical pulse code modulation (PCM) severely errored second.

5. SDP Signaling

[RFC3611] defines the use of SDP (Session Description Protocol) [RFC4566] for signaling the use of XR blocks. XR blocks MAY be used without prior signaling.

5.1. SDP rtcp-xr Attribute Extension

This section augments the SDP [RFC4566] attribute "rtcp-xr" defined in [RFC3611] by providing an additional value of "xr-format" to signal the use of the report block defined in this document. The ABNF [RFC5234] syntax is as follows.

```
xr-format =/ xr-ind-bgd-block

xr-ind-bgd-block = "ind-burst-gap-discard"
```

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 in Offer/Answer for unilateral parameters, refer to Section 5.2 of [RFC3611].

6. 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].

6.1. New RTCP XR Block Type Value

This document assigns the block type value IBGD in the IANA "RTP Control Protocol Extended Reports (RTCP XR) Block Type Registry" to the "Burst/Gap Discard Metrics Block".

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

6.2. New RTCP XR SDP Parameter

This document also registers a new parameter "ind-burst-gap-discard" in the "RTP Control Protocol Extended Reports (RTCP XR) Session Description Protocol (SDP) Parameters Registry".

6.3. Contact Information for Registrations

The contact information for the registrations is:

RAI Area Directors <rai-ads@tools.ietf.org>

7. 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 confidentiality documented in Section 7, paragraph 3 of [RFC3611] does not apply.

8. Contributors

Qin Wu, Rachel Huang, and Alan Clark wrote RFC7003, which this document extends.

9. Acknowledgments

The authors acknowledge the reviews and feedback provided by various people.

10. References

10.1. 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.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[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, February 2010.

[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, October 2012.

10.2. Informative References

[I-D.ietf-payload-flexible-fec-scheme] Singh, V., Begen, A., Zanaty, M., and G. Mandyam, "RTP Payload Format for Flexible Forward Error Correction (FEC)", draft-ietf-payload-flexible-fec-scheme-01 (work in progress), October 2015.

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

[RFC5481] Morton, A. and B. Claise, "Packet Delay Variation Applicability Statement", RFC 5481, DOI 10.17487/RFC5481, March 2009, <http://www.rfc-editor.org/info/rfc5481>.

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

[RFC6709] Carpenter, B., Aboba, B., Ed., and S. Cheshire, "Design Considerations for Protocol Extensions", RFC 6709, DOI 10.17487/RFC6709, September 2012, <http://www.rfc-editor.org/info/rfc6709>.

[RFC6792] Wu, Q., Ed., Hunt, G., and P. Arden, "Guidelines for Use of the RTP Monitoring Framework", RFC 6792, DOI 10.17487/RFC6792, November 2012, <http://www.rfc-editor.org/info/rfc6792>.

[RFC6958] Clark, A., Zhang, S., Zhao, J., and Q. Wu, "RTP Control Protocol (RTCP) Extended Report (XR) Block for Burst/Gap Loss Metric Reporting", RFC 6958, May 2013.

[RFC7002] Clark, A., Zorn, G., and Q. Wu, "RTP Control Protocol (RTCP) Extended Report (XR) Block for Discard Count Metric Reporting", RFC 7002, September 2013.

[RFC7003] Clark, A., Huang, R., and Q. Wu, "RTP Control Protocol (RTCP) Extended Report (XR) Block for Burst/Gap Discard Metric Reporting", RFC 7003, September 2013.

Appendix A. Metrics Represented Using the Template from RFC 6390

a. Threshold Metric

   * Defined in Appenix A.a of [RFC7003].

b. Sum of burst durations (ms)

   * Metric Name: Sum of Burst Durations with Discarded RTP Packets.

   * Metric Description: The total duration of bursts of discarded RTP packets in the period of the report.

   * Method of Measurement or Calculation: See Section 3.1, Sum of Burst Durations definition.

   * Units of Measurement: See Section 3.1, Sum of Burst Durations definition.

   * Measurement Point(s) with Potential Measurement Domain: See Section 3, 1st paragraph.

   * Measurement Timing: See Section 3, 2nd paragraph for measurement timing and Section 3.1 for Interval Metric flag.

   * Use and Applications: See Section 1.4.

   * Reporting Model: See RFC 3611.

c. Packets Discarded in Bursts Metric

   * Defined in Appenix A.b of [RFC7003].

d. Number of bursts

   * Metric Name: Number of discard bursts in RTP.

   * Metric Description: The total number of bursts with discarded RTP packets in the period of the report.

   * Method of Measurement or Calculation: See Section 3.1, Number of discard bursts definition.

   * Units of Measurement: See Section 3.1 for the Number of bursts definition.

   * Measurement Point(s) with Potential Measurement Domain: See Section 3, 1st paragraph.

   * Measurement Timing: See Section 3, 2nd paragraph for measurement timing and Section 3.1 for Interval Metric flag.

   * Use and Applications: See Section 1.4.

   * Reporting Model: See RFC 3611.

e. Total Packets Expected in Bursts Metric

   * Defined in Appenix A.c of [RFC7003].

f. Discard Count

   * Defined in Appenix A.a of [RFC7002].

Authors' Addresses

Varun Singh (editor)
Nemu Dialogue Systems Oy
Runeberginkatu 4c A 4
Helsinki 00100
Finland

EMail: varun@callstats.io
URI: http://www.callstats.io/

Colin Perkins
University of Glasgow
School of Computing Science
Glasgow G12 8QQ
United Kingdom

EMail: csp@csperkins.org

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

EMail: alan.d.clark@telchemy.com

Rachel Huang
Huawei Technologies Co., Ltd.
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012
China

EMail: Rachel@huawei.com