

AVT
Internet-Draft
Updates: [3550](#) (if approved)
Intended status: Standards Track
Expires: December 4, 2008

J. Lennox
Vidyo
T. Schierl
Fraunhofer HHI
S. Ganesan
Motorola
June 2, 2008

Real-Time Transport Protocol (RTP) Timestamps for Layered Encodings
draft-lennox-avt-rtp-layered-encoding-timestamps-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of 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/ietf/lid-abstracts.txt>.

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

This Internet-Draft will expire on December 4, 2008.

Abstract

The Real-Time Transport Protocol (RTP) specification defines how layered encodings can be sent over a layered transmission system. A source can stripe the progressive layers of a hierarchically represented signal across multiple RTP sessions, each carried on, for example, its own multicast group. These layered encodings are given special treatment in RTP, notably in that the same synchronization source (SSRC) identifier space is used across the sessions of all layers.

The RTP protocol specification does not, however, explicitly state how RTP timestamps are to be used with layered encodings. This document updates the RTP specification to require that RTP timestamps for layered encodings be synchronized, i.e. that every layer chooses the same random initial value for the timestamp.

Table of Contents

1.	Introduction	3
2.	Terminology	3
3.	Normative Requirements	3
4.	Discussion	3
5.	Architectural Implications	4
6.	Payload Design Considerations	5
7.	Security Considerations	5
8.	IANA Considerations	5
9.	References	6
9.1.	Normative References	6
9.2.	Informative References	6
	Authors' Addresses	7
	Intellectual Property and Copyright Statements	8

1. Introduction

The Real-Time Transport Protocol (RTP) [[RFC3550](#)] specification defines how layered encodings can be sent over a layered transmission system. A source can stripe the progressive layers of a hierarchically represented signal across multiple RTP sessions, each carried on, for example, its own multicast group. These layered encodings are given special treatment in RTP, notably in that the same synchronization source (SSRC) identifier space is used across the sessions of all layers.

The RTP protocol specification does not, however, explicitly state how RTP timestamps are to be used with layered encodings. This document updates the RTP specification to require that RTP timestamps for layered encodings be synchronized, i.e. that every layer chooses the same random initial value for the timestamp.

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](#)] and indicate requirement levels for compliant implementations.

3. Normative Requirements

When a source is sent as a layered encoding transmitted on separate RTP sessions (as defined in [Section 2.4 of \[RFC3550\]](#)), such that the same synchronization source (SSRC) identifier is used on each session, the same initial (random) RTP timestamp value MUST be used for every layer.

(Since each layer's RTP timestamps are derived from the same media clock, and so will advance at the same rate, this implies that RTP

packets will have equal timestamps if they are (logically) generated at once, e.g., belong to the same video frame, as with packets on a single session.)

4. Discussion

Speer and McCanne [[I-D.speer-avt-layered-video](#)] defined how layered encoding support would be added to the original RTP specification [[RFC1889](#)]. This work was adapted into the current RTP specification when it was revised [[RFC3550](#)].

This specification modified RTP so that the same synchronization source (SSRC) identifier would be used on each session for a layered encoding transmitted on multiple streams. As discussed in that draft, the alternative would be to allocate each layer's SSRC independently, and associate the streams using the canonical name (CNAME) information sent periodically in RTCP source description (SDES) packets, as RTP does to associate separate audio and video streams from a single user. However, this alternative introduces additional complexity, in that it forces each receiver to manage all the CNAME/SSRC bindings; requires newly-arrived receivers to wait for the source description packets before they can start decoding a stream; and creates new error recovery conditions for dealing with conflicting information that arrives on the different sessions.

Speer and McCanne specification's did not say anything about RTP timestamps. However, as documented in McCanne's Ph.D. Thesis [[McCa96](#)], vic [[VIC](#)], the primary implementation of layered encoding of RTP, sent base and enhancement layers of a video stream with synchronized RTP timestamps, and relied on this fact to associate the frames when decoding them.

Absent payload-specific synchronization information, as with source identifiers, the alternative for stream alignment would be to rely on RTCP reports, in this case on the NTP timestamps carried in carried in RTCP sender report (SR) packets. However, this would introduce much the same problems as relying on CNAME-based synchronization for the sources. It introduces significant additional complexity; receivers must wait for the receipt of SR packets before they can start decoding a stream; and conflicting information can arise from

the different sessions, particularly for sessions with long RTCP reporting intervals if there is clock skew between a source's NTP and media timestamps. This largely removes any advantage of SSRC synchronization across the layers.

[5.](#) Architectural Implications

RTP timestamp randomization has two primary motivations: it improves the probability of detection of SSRC collisions, and it provides additional randomness for [[RFC3550](#)]-style packet encryption (a "weak initialization vector", in the words of that RFC).

Synchronizing RTP timestamps across sessions does not harm SSRC collision detection. As specified by [[RFC3550](#)], for layered sessions the base layer's session is used for SSRC identifier allocation and collision resolution. When two sources collide, they will collide on every session layer on which they are being sent; and when a source changes its SSRC following a collision, it will change it on every

session.

The security implications of timestamp synchronization are discussed in [Section 7](#).

[6.](#) Payload Design Considerations

Depending on the payload, RTP timestamp synchronization may not be sufficient to completely reconstruct the order in which packets sent over several RTP sessions need to be decoded. In such cases, the payload definition needs to specify how the decoding order of packets is reconstructed.

Difficulties particularly arise if if a payload allows packets with a given timestamp to be omitted on some sessions; if a payload has non-trivial decoding order constraints for media with the same timestamp; or if a payload supports a transmission order different from its timestamp order, as is common with video formats.

[7.](#) Security Considerations

For [\[RFC3550\]](#)-style packet encryption, RTP timestamp randomization contributes to a "weak initialization vector" for encrypted packets. In particular, the timestamp, sequence number, and SSRC together provide randomness to a session.

However, when timestamps and sequence numbers are aligned across multiple sessions, for many payloads sequence numbers will also align periodically (if packets are sent at different rates on each session.) This introduces a weakness which can allow an attacker to launch "two-time-pad" attacks against the bitstream. Thus, if [\[RFC3550\]](#)-style RTP packet encryption is used to protect a layered encoding, different encryption keys MUST be used on each RTP session of the layered encoding.

For Secure RTP (SRTP) [\[RFC3711\]](#), similarly, a different SRTP master key MUST be used for each RTP session. The key management mechanisms Secure Descriptions for SDP [\[RFC4568\]](#), Key Management Extensions for SDP and RTSP [\[RFC4567\]](#) combined with MIKEY [\[RFC3830\]](#), DTLS-SRTP [\[I-D.ietf-sip-dtls-srtp-framework\]](#), and ZRTP [\[I-D.zimmermann-avt-zrtp\]](#) all satisfy this requirement.

[8.](#) IANA Considerations

No action by IANA is required.

[9.](#) References

[9.1.](#) 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.
- [RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", [RFC 3711](#), March 2004.

[9.2.](#) Informative References

- [I-D.ietf-sip-dtls-srtp-framework]
Fischl, J., Tschofenig, H., and E. Rescorla, "Framework for Establishing an SRTP Security Context using DTLS", [draft-ietf-sip-dtls-srtp-framework-01](#) (work in progress), February 2008.
- [I-D.speer-avt-layered-video]
Speer, M. and S. McCanne, "RTP usage with Layered Multimedia Streams", [draft-speer-avt-layered-video-05](#) (work in progress), June 1997.
- Expired draft.
- [I-D.zimmermann-avt-zrtp]
Zimmermann, P., Johnston, A., and J. Callas, "ZRTP: Media Path Key Agreement for Secure RTP", [draft-zimmermann-avt-zrtp-06](#) (work in progress), March 2008.
- [McCa96] McCanne, S., "Scalable Compression and Transmission of Internet Multicast Video", Report No. UCB/CSD-96-928, December 1996.
- Ph.D. Dissertation, University of California Berkeley.
- [RFC1889] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", [RFC 1889](#), January 1996.
- [RFC3830] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", [RFC 3830](#),

August 2004.

- [RFC4567] Arkko, J., Lindholm, F., Naslund, M., Norrman, K., and E. Carrara, "Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)", [RFC 4567](#), July 2006.
- [RFC4568] Andreasen, F., Baugher, M., and D. Wing, "Session

Description Protocol (SDP) Security Descriptions for Media Streams", [RFC 4568](#), July 2006.

[VIC] McCanne, S. and V. Jacobson, "vic: A Flexible Framework for Packet Video", 1995.

ACM Multimedia, pp. 511-522

Authors' Addresses

Jonathan Lennox
Vidyo, Inc.
433 Hackensack Avenue
Sixth Floor
Hackensack, NJ 07601
US

Email: jonathan@vidyo.com

Thomas Schierl
Fraunhofer HHI
Einsteinufer 37
D-10587 Berlin
Germany

Phone: +49-30-31002-227
Email: schierl@hhi.fhg.de

Sam Ganesan
Motorola
80 Central Street
Buxborough, MA 01719
US

Email: sam.ganesan@motorola.com

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.