AVT
Internet-Draft
Expires: November 18, 2005

F. Andreasen
D. Oran
D. Wing
Cisco Systems, Inc.
May 17, 2005

A No-Op Payload Format for RTP
draft-wing-avt-rtp-noop-03

Status of this Memo

Copyright Notice

Abstract

This document defines an no-op payload format for the Real-time Transport Protocol (RTP), and a mechanism to request transmission of an early RTCP report. This can be used to verify RTP connectivity and to keep Network Address Translator (NAT) bindings and Firewall pinholes open.

Table of Contents

1. Introduction

This memo defines a new RTP payload format called "no-op". This payload behaves like a normal RTP payload, except the RTP packet is not used to play out media. It is also explicitly designed to interact constructively with the RTCP feedback profile [6].

This new payload format is useful for:

- media session reception quality assessment, such as at the beginning of a session;
- keepalives to keep NAT bindings and/or firewall pinholes open when RTP media traffic is not otherwise being transmitted.

In addition it has a number of uses whose utility is speculative but for which it is easy pressed into service:

- measurement-based admission control by probing available bandwidth, and
- synthetic load generation for performance testing and other minimally-intrusive instrumentation.

When an endpoint mas a media stream marked as 'recvonly' or 'inactive' the endpoint is not supposed to send any media (i.e. RTP packets). However, to keep a NAT binding alive, the endpoint will need to send packets over the RTP and RTCP ports. RTP No-Op is ideally suited to this. In comparison, if one participant in an audio multicast conference has a 'recvonly' or 'inactive' media stream yet occasionally sends comfort noise packets in order to keep its NAT binding open, these comfort noise packets are interpreted as audio packets by receivers and mixers which can cause undesirable behavior -- such as selection of the primary speaker or the playout of comfort noise when no audio should be played.

Unlike Comfort noise [9], which is specific to voice RTP streams, RTP No-Op is applicable to any kind of RTP stream including video, audio, realtime text, or any other media type that would benefit from the capabilities listed above. This gives RTP No-Op an advantage as a NAT keepalive mechanism. Certain functions and RTP payload types can use RTP No-Op without re-inventing their own payload-specific NAT keepalive mechanism -- such as video muting, Clearmode [10], and text [11].

Some audio codecs have their own 'silence' packets. However, some codecs only send such 'silence' packets if the noise floor changes; G.729b [12] is an example of such a codec. RTP No-Op allows the RTP stack itself, rather than the codec, to send periodic packets as a keepalive mechanism.

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 [1].

2. RTP Payload Format for No-Op

2.1 Registration

The RTP payload format is designated as "no-op" and the MIME types are "audio/no-op", "video/no-op", and "text/no-op". The default clock rate is 8000 Hz, but other rates MAY be used. In accordance with current practice, this payload format does not have a static payload type number, but uses a RTP payload type number established dynamically out-of-band, e.g. through SDP [4].

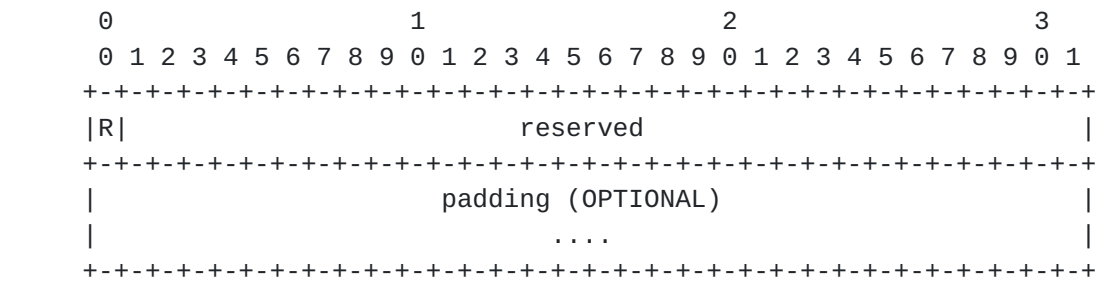
2.2 Use of RTP Header Fields

Timestamp: The RTP timestamp reflects the measurement point for the current packet. The receiver calculates jitter for RTCP receiver reports based on all packets with a given timestamp. Note: The jitter value should primarily be used as a means for comparing the reception quality between two users or two time-periods, not as an absolute measure.

Marker bit: The RTP marker bit has no special significance for this payload type.

2.3 Payload Format

The payload format is shown below.



The payload contains at least 4 bytes. The first 32 bits are defined as follows:

bit 0: "R", "Request Early RTCP", is used to request invocation of RTCP feedback by timely transmission of an RTCP report (see Section 2.6).

bits 1-31: Reserved; contents are ignored.

Additional padding bytes MAY be appended up to the ptime value in SDP (see Section 2.7). These bytes are ignored. Padding may be useful to generate RTP packets that are the same size as a normal media payload.

2.4 Sender Operation

As discussed in the introduction, endpoints MUST occasionally send a packet to their RTP and RTCP peer to keep NAT and firewall bindings active, even if the media stream is marked 'recvonly' or 'inactive'. If no other RTP packet has been sent for approximately 30 seconds, an RTP NoOp packet SHOULD be sent. It is permissible to send a NoOp packet even for media streams marked 'recvonly' or 'inactive'.

2.5 Mixer, Translator Operation

An RTP mixer or unicast-to-unicast RTP translator SHOULD forward RTP No-Op payload packets normally. A unicast-to-multicast RTP translator SHOULD replicate RTP No-Op payload packets normally.

A multicast-to-unicast RTP translator SHOULD NOT replicate an RTP No-Op packet with the Request Early RTCP bit set unless:

1. all receivers are known to be operating under the bandwidth limitations rules of [6], and
2. the restriction of applicability to "small groups" in [6] is observed

Otherwise the sender may be flooded with RTCP reports.

2.6 Receiver Operation

Upon receipt of an RTP packet with the No-Op payload format and the 'Request Early RTCP Report' bit set to 0, the receiver performs normal RTP receive operations on it -- incrementing the RTP receive counter, calculating jitter, and so on. The receiver then discards the packet -- it is not used to play out media.

Upon receipt of an RTP packet with the No-Op payload format and the 'Request Early RTCP Report' bit set to 1, the receiver adjusts counters as described above and then also performs the following steps (with reference to the definitions and procedures of the AVPF profile [6]):

1. ascertains whether the associated RTP session is operating under the AVPF RTP profile (or one derived from it via combination with another RTP profile). If not the receiver takes no further

action on this packet - specifically, if the RTP/AVPF profile (or one derived from it) is not used the receiver MUST NOT send an early RTCP report. If so, it continues as follows.

2. generates a feedback "Event" which in turn may trigger the generation of a "FB message".
3. sends the FB message as an "early RTCP packet" assuming the bandwidth constraints for feedback messages are satisfied.
4. Otherwise, takes no further action

2.7 Indication of No-OP Capability using SDP

Senders and receivers may indicate support for the No-Op payload format, for example, by using the Session Description Protocol SDP [4]. If the payload format is being used for connectivity verification (e.g. in conjunction with [5]) senders and receivers MUST advertise the AVPF profile (or a profile used in combination with it).

The default packetization interval for this payload type is 20ms (ptime:20) but alternate values can be advertised in SDP using the ptime attribute value [4].

3. Example SDP Offer/Answer

Offer:

```
v=0
o=alice 2890844526 2890844526 IN IP4 host.atlanta.example.com
s=-
c=IN IP4 host.atlanta.example.com
t=0 0
m=audio 49170 RTP/AVPF 0 33
a=rtpmap:0 PCMU/8000
a=rtpmap:33 no-op/8000
m=video 41372 RTP/AVPF 31 36
a=rtpmap:31 H261/90000
a=rtpmap:36 no-op/90000
```

```
Answer:
      v=0
      o=bob 2808844564 2808844564 IN IP4 host.biloxi.example.com
      s=-
      c=IN IP4 host.biloxi.example.com
      t=0 0
      m=audio 59174 RTP/AVPF 0 33
      a=rtpmap:0 PCMU/8000
      a=rtpmap:33 no-op/8000
      m=video 59170 RTP/AVPF 32 36
      a=rtpmap:31 H261/90000
      a=rtpmap:36 no-op/90000
```

4. MIME Registration

This section registers MIME types for audio/no-op, video/no-op, and text/no-op.

4.1 audio/no-op

MIME media type name: audio

MIME subtype name: no-op

Required parameters: none

Optional parameters: none

Encoding considerations: This type is only defined for transfer via RTP [2] and Secure RTP [3].

Security considerations: See Section 5, "Security Considerations", in this document.

Interoperability considerations: none

Published specification: This document.

Applications which use this media: The "no-op" application subtype is used to maintain network state or verify network connectivity, when a more traditional RTP payload type cannot be used.

Additional information:

1. Magic number(s): N/A
2. File extension(s): N/A

3. Macintosh file type code: N/A

4.2 video/no-op

MIME media type name: video

MIME subtype name: no-op

Required parameters: none

Optional parameters: none

Encoding considerations: This type is only defined for transfer via RTP [2] and Secure RTP [3].

Security considerations: See Section 5, "Security Considerations", in this document.

Interoperability considerations: none

Published specification: This document.

Applications which use this media: The "no-op" application subtype is used to maintain network state or verify network connectivity, when a more traditional RTP payload type cannot be used.

Additional information:

1. Magic number(s): N/A
2. File extension(s): N/A
3. Macintosh file type code: N/A

4.3 text/no-op

MIME media type name: text

MIME subtype name: no-op

Required parameters: none

Optional parameters: none

Encoding considerations: This type is only defined for transfer via RTP [2] and Secure RTP [3].

Security considerations: See Section 5, "Security Considerations", in this document.

Interoperability considerations: none

Published specification: This document.

Applications which use this media: The "no-op" application subtype is used to maintain network state or verify network connectivity, when a more traditional RTP payload type cannot be used.

Additional information:

1. Magic number(s): N/A
2. File extension(s): N/A
3. Macintosh file type code: N/A

5. Security Considerations

Without security of the RTP stream (via SRTP [3], IPsec [8], or other means), it is possible for an attacker to spoof RTP packets, including this new packet type. As this new RTP payload type includes a method to request early transmission of RTCP, this could be used to cause endpoints to flood the network with RTCP reports. Thus, the RTCP transmissions MUST NOT exceed the bandwidth recommendations described in section 6.3 of RFC3550 [2].

6. IANA Considerations

IANA is requested to make MIME type registrations as specified above in Section 4

7. Acknowledgments

Thanks to Henning Schulzrinne for suggesting using RTCP as a feedback mechanism.

8. References

8.1 Normative References

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

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

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

[4] Handley, M. and V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.

[5] Andreasen, F., "Connectivity Preconditions for Session Description Protocol Media Streams", draft-andreasen-mmusic-connectivityprecondition-02 (work in progress), February 2005.

[6] Ott, J. and S. Wenger, "Extended RTP Profile for RTCP-based Feedback(RTP/AVPF)", draft-ietf-avt-rtcp-feedback-11 (work in progress), August 2004.

[7] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Multimedia Session Establishment Protocols", draft-ietf-mmusic-ice-04 (work in progress), February 2005.

8.2 Informational References

[8] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[9] Zopf, R., "Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)", RFC 3389, September 2002.

[10] Kreuter, R., "RTP Payload Format for a 64 kbit/s Transparent Call", RFC 4040, April 2005.

[11] Hellstrom, G., "RTP Payload for Text Conversation", RFC 2793, May 2000.

[12] International Telecommunications Union, "G.729 Annex B", November 1999, <http://www.itu.int/ITU-T/publications/recs.html>.

Authors' Addresses

Flemming Andreasen
Cisco Systems, Inc.
499 Thornall Street, 8th Floor
Edison, NJ 08837
USA

Email: fandreas@cisco.com

David Oran
Cisco Systems, Inc.
7 Ladyslipper Lane
Acton, MA 01720
USA

Email: oran@cisco.com

Dan Wing
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

Email: dwing@cisco.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.