Network Working Group   M. Westerlund
Internet-Draft   B. Burman
Intended status: Standards Track   Ericsson
Expires: December 12, 2016   R. Even
                                                 Huawei Technologies
                                                          M. Zanaty
                                                      Cisco Systems
                                                      June 10, 2016

           RTP Header Extension for RTCP Source Description Items
                    draft-ietf-avtext-sdes-hdr-ext-07

Abstract

   Source Description (SDES) items are normally transported in RTP
   control protocol (RTCP). In some cases it can be beneficial to speed
   up the delivery of these items. Mainly when a new source (SSRC)
   joins an RTP session and the receivers need this source's identity,
   relation to other sources, or its synchronization context, all of
   which may be fully or partially identified using SDES items. To
   enable this optimization, this document specifies a new RTP header
   extension that can carry SDES items.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This specification defines an RTP header extension [RFC3550][RFC5285]
that can carry RTCP source description (SDES) items. Normally the
SDES items are carried in their own RTCP packet type [RFC3550]. By
including selected SDES items in a header extension the determination
of relationship and synchronization context for new RTP streams
(SSRCs) in an RTP session can be optimized. Which relationship and
what information depends on the SDES items carried. This becomes a
complement to using only RTCP for SDES Item delivery.

It is important to note that not all SDES items are appropriate to
transmit using RTP header extensions. Some SDES items performs
binding or identifies synchronization context with strict timeliness
requirements, while many other SDES items do not have such
requirements. In addition, security and privacy concerns for the
SDES item information need to be considered. For example, the Name
and Location SDES items are highly sensitive from a privacy
perspective and should not be transported over the network without
strong security. No use case has identified where this information
is required at the same time as the first RTP packets arrive. A few
seconds delay before such information is available to the receiver
appears acceptable. Therefore only appropriate SDES items will be
registered for use with this header extension, such as CNAME.

First, some requirements language and terminology are defined. The
following section motivates why this header extension is sometimes
required or at least provides a significant improvement compared to
waiting for regular RTCP packet transmissions of the information.
This is followed by a specification of the header extension and usage
recommendations. Next, a sub-space of the header-extension URN is
defined to be used for existing and future SDES items, and then the
appropriate existing SDES items are registered.

2. Definitions

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in RFC 2119 [RFC2119].

2.2. Terminology

This document uses terminology defined in "A Taxonomy of Semantics
and Mechanisms for Real-Time Transport Protocol (RTP) Sources"
[RFC7656]. In particular the following definitions:

    Media Source

    RTP Stream

    Media Encoder

    Participant

3. Motivation

   Source Description (SDES) items are associated with a particular SSRC
   and thus RTP stream. The source description items provide various
   meta data associated with the SSRC. How important it is to have this
   data no later than when receiving the first RTP packets depends on
   the item itself. The CNAME item is one item that is commonly needed
   either at reception of the first RTP packet for this SSRC, or at
   least by the time the first media can be played out. If it is not
   available, the synchronization context cannot be determined and thus
   any related streams cannot be correctly synchronized. Thus, this is
   a valuable example for having this information early when a new RTP
   stream is received.

   The main reason for new SSRCs in an RTP session is when media sources
   are added. This can be either because an end-point is adding a new
   actual media source, or additional participants in a multi-party
   session are added to the session. Another reason for a new SSRC can
   be an SSRC collision that forces both colliding parties to select new
   SSRCs.

   For the case of rapid media synchronization, one may use the RTP
   header extension for Rapid Synchronization of RTP Flows [RFC6051].
   This header extension carries the clock information present in the
   RTCP sender report (SR) packets. It however assumes that the CNAME
   binding is known, which can be provided via signaling [RFC5576] in
   some cases, but not all. Thus an RTP header extension for carrying
   SDES items like CNAME is a powerful combination to enable rapid
   synchronization in all cases.

   The Rapid Synchronization of RTP Flows specification does provide an
   analysis of the initial synchronization delay for different sessions
   depending on number of receivers as well as on session bandwidth
   (Section 2.1 of [RFC6051]). These results are applicable also for
   other SDES items that have a similar time dependency until the
   information can be sent using RTCP. These figures can be used to
   determine the benefit of reducing the initial delay before
   information is available for some use cases.

   Rapid Synchronization of RTP Flows [RFC6051] also discusses the case
   of late joiners, and defines an RTCP Feedback format to request
   synchronization information, which is another potential use case for
   SDES items in RTP header extension. It would for example be natural
   to include CNAME SDES item with the header extension containing the
   NTP formatted reference clock to ensure synchronization.

   The ongoing work on bundling SDP media descriptions
   [I-D.ietf-mmusic-sdp-bundle-negotiation] has identified a new SDES

item that can benefit from timely delivery. A corresponding RTP SDES
compact header extension is therefore also defined and registered in
that document:

MID: This is a media description identifier that matches the value
   of the Session Description Protocol (SDP) [RFC4566] a=mid
   attribute [RFC5888], to associate RTP streams multiplexed on the
   same transport with their respective SDP media description.

4. Specification

This section first specifies the SDES item RTP header extension
format, followed by some usage considerations.

4.1. SDES Item Header Extension

An RTP header extension scheme allowing for multiple extensions is
defined in "A General Mechanism for RTP Header Extensions" [RFC5285].
That specification defines both short and long item headers. The
short headers (One-byte) are restricted to 1 to 16 bytes of data,
while the long format (Two-byte) supports a data length of 0 to 255
bytes. Thus the RTP header extension formats are capable of
supporting any SDES item from a data length perspective.

The ID field, independent of short or long format, identifies both
the type of RTP header extension and, in the case of the SDES item
header extension, the type of SDES item. The mapping is done in
signaling by identifying the header extension and SDES item type
using a URN, which is defined in the IANA consideration (Section 5)
for the known SDES items appropriate to use.

4.1.1. One-Byte Format

The one-byte header format for an SDES item extension element
consists of the one-byte header (defined in Section 4.2 of
[RFC5285]), which consists of a 4-bit ID followed by a 4-bit length
field (len) that identifies the number of data bytes (len value +1)
following the header. The data part consists of len+1 bytes of UTF-8
[RFC3629] text. The type of text and its mapping to the SDES item
type is determined by the ID field value.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  ID   |  len  | SDES Item text value ...                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
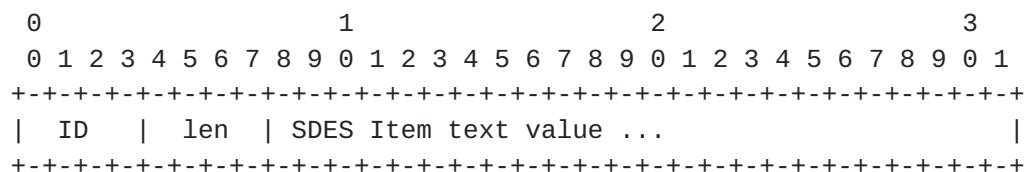
Figure 1

4.1.2. Two-Byte Format

The two-byte header format for an SDES item extension element
consists of the two-byte header (defined in Section 4.3 of
[RFC5285]), which consists of an 8-bit ID followed by an 8-bit length
field (len) that identifies the number of data bytes following the
header. The data part consists of len bytes of UTF-8 text. The type
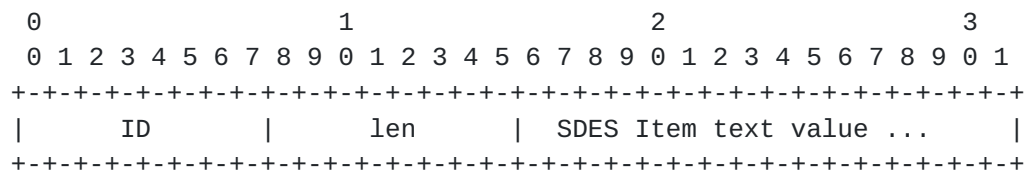of text and its mapping to the SDES item type is determined by the ID
field value.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      ID       |     len       |   SDES Item text value ...    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2

4.2. Usage of the SDES Item Header Extension

This section discusses various usage considerations; which form of
header extension to use, the packet expansion, and when to send SDES
items in header extension.

4.2.1. One or Two Byte Headers

The RTP header extensions for SDES items MAY use either the one-byte
or two-byte header formats, depending on the text value size for the
used SDES items and the requirement from any other header extensions
used. The one-byte header SHOULD be used when all non SDES item
header extensions supports the one-byte format and all SDES item text
values contain at most 16 bytes. Note that the RTP header extension
specification does not allow mixing one-byte and two-byte headers for
the same RTP stream (SSRC), so if the value size of any of the SDES
items value requires the two-byte header, then all other header
extensions MUST also use the two-byte header format.

For example using CNAMEs that are generated according to "Guidelines
for Choosing RTP Control Protocol (RTCP) Canonical Names (CNAMEs)"
[RFC7022], using short term persistent values, and if 96-bit random
values prior to base64 encoding are sufficient, then they will fit
into the one-byte header format.

An RTP middlebox needs to take care choosing between one-byte headers
and two-byte headers when creating the first packets for an outgoing
stream (SSRC) with header extensions. First of all it needs to
consider all the header extensions that may potentially be used.
Secondly, it needs to know the size of the SDES items that are going

   to be included, and use two bytes headers if any are longer than 16
   bytes. An RTP middlebox that forwards a stream, i.e., not mixing it
   or combing it with other streams, may be able to base its choice on
   the header size in incoming streams. This is assuming that the
   middlebox does not modify the stream or add additional header
   extensions to the stream it sends, in which case it needs to make its
   own decision.

4.2.2. MTU and Packet Expansion

   The RTP packet size will clearly increase when a header extension is
   included. How much depends on the type of header extensions and
   their data content. The SDES items can vary in size. There are also
   some use-cases that require transmitting multiple SDES items in the
   same packet to ensure that all relevant data reaches the receiver.
   An example of that is when both CNAME, a MID, and the rapid time
   synchronization extension from RFC 6051 are needed. Such a
   combination is quite likely to result in at least 16+3+8 bytes of
   data plus the headers, which will be another 7 bytes for one-byte
   headers, plus two bytes of header padding to make the complete header
   extension 32-bit word aligned, thus in total 36 bytes.

   If the packet expansion cannot be taken into account when producing
   the RTP payload, it can cause an issue. An RTP payload that is
   created to meet a particular IP level Maximum Transmission Unit
   (MTU), taking the addition of IP/UDP/RTP headers but not RTP header
   extensions into account, could exceed the MTU when the header
   extensions are present, thus resulting in IP fragmentation. IP
   fragmentation is known to negatively impact the loss rate due to
   middleboxes unwilling or not capable of dealing with IP fragments, as
   well as increasing the target surface for other types of packet
   losses.

   As this is a real issue, the media encoder and payload packetizer
   should be flexible and be capable of handling dynamically varying
   payload size restrictions to counter the packet expansion caused by
   header extensions. If that is not possible, some reasonable worst
   case packet expansion should be calculated and used to reduce the RTP
   payload size of all RTP packets the sender transmits.

4.2.3. Transmission Considerations

   The general recommendation is to only send header extensions when
   needed. This is especially true for SDES items that can be sent in
   periodic repetitions of RTCP throughout the whole session. Thus, the
   different usages (Section 4.2.4) have different recommendations.
   First some general considerations for getting the header extensions
   delivered to the receiver:

1. The probability for packet loss and burst loss determine how many
    repetitions of the header extensions will be required to reach a
    targeted delivery probability, and if burst loss is likely, what
    distribution would be needed to avoid getting all repetitions of
    the header extensions lost in a single burst.

2. If a set of packets are all needed to enable decoding, there is
    commonly no reason for including the header extension in all of
    these packets, as they share fate. Instead, at most one instance
    of the header extension per independently decodable set of media
    data would be a more efficient use of the bandwidth.

3. How early the SDES item information is needed, from the first
    received RTP data or only after some set of packets are received,
    can guide if the header extension(s) should be in all of the
    first N packets or be included only once per set of packets, for
    example once per video frame.

4. The use of RTP level robustness mechanisms, such as RTP
    retransmission [RFC4588], or Forward Error Correction, e.g.,
    [RFC5109] may treat packets differently from a robustness
    perspective, and SDES header extensions should be added to
    packets that get a treatment corresponding to the relative
    importance of receiving the information.

As a summary, the number of header extension transmissions should be
tailored to a desired probability of delivery taking the receiver
population size into account. For the very basic case, N repetitions
of the header extensions should be sufficient, but may not be
optimal. N is selected so that the header extension target delivery
probability reaches $1-P^N$, where P is the probability of packet loss.
For point to point or small receiver populations, it might also be
possible to use feedback, such as RTCP, to determine when the
information in the header extensions has reached all receivers and
stop further repetitions. Feedback that can be used includes the
RTCP XR Loss RLE report block [RFC3611], which will indicate
successful delivery of particular packets. If the RTP/AVPF Transport
Layer Feedback Messages for generic NACK [RFC4585] is used, it can
indicate the failure to deliver an RTP packet with the header
extension, thus indicating the need for further repetitions. The
normal RTCP report blocks can also provide an indicator of successful
delivery, if no losses are indicated for a reporting interval
covering the RTP packets with the header extension. Note that loss
of an RTCP packet reporting on an interval where RTP header extension
packets were sent, does not necessarily mean that the RTP header
extension packets themselves were lost.

4.2.4. Different Usages

4.2.4.1. New SSRC

A new SSRC joins an RTP session. As this SSRC is completely new for
everyone, the goal is to ensure, with high probability, that all RTP
session participants receives the information in the header
extension. Thus, header extension transmission strategies that allow
some margins in the delivery probability should be considered.

4.2.4.2. Late Joiner

In a multi-party RTP session where one or a small number of receivers
join a session where the majority of receivers already have all
necessary information, the use of header extensions to deliver
relevant information should be tailored to reach the new receivers.
The trigger to send header extensions can for example either be RTCP
from new receiver(s) or an explicit request like the Rapid
Resynchronization Request defined in [RFC6051]. In centralized
topologies where an RTP middlebox is present, it can be responsible
for transmitting the known information, possibly stored, to the new
session participant only, and not repeat it to all the session
participants.

4.2.4.3. Information Change

If the SDES information is tightly coupled with the RTP data, and the
SDES information needs to be updated, then the use of the RTP header
extension is superior to RTCP. Using the RTP header extension
ensures that the information is updated on reception of the related
RTP media, ensuring synchronization between the two. Continued use
of the old SDES information can lead to undesired effects in the
application. Thus, header extension transmission strategies with
high probability of delivery should be chosen.

4.2.5. SDES Items in RTCP

The RTP header extension information, i.e., SDES items, can and will
be sent also in RTCP. Therefore, it is worth making some reflections
on this interaction. As an alternative to the header extension, it
is possible to schedule a non-regular RTCP packet transmission
containing important SDES items, if one uses an RTP/AVPF-based RTP
profile. Depending on which mode one's RTCP feedback transmitter is
working on, extra RTCP packets may be sent as immediate or early
packets, enabling more timely SDES information delivery.

There are however two aspects that differ between using RTP header
extensions and any non-regular transmission of RTCP packets. First,

as the RTCP packet is a separate packet, there is no direct relation
and also no fate sharing between the relevant media data and the SDES
information. The order of arrival for the packets will matter. With
a header-extension, the SDES items can be ensured to arrive if the
media data to play out arrives. Secondly, it is difficult to
determine if an RTCP packet is actually delivered. This, as the RTCP
packets lack both sequence number and a mechanism providing feedback
on the RTCP packets themselves.

4.2.6. Update Flaps

The SDES item may arrive both in RTCP and in RTP header extensions,
potentially causing the value to flap back and forth at the time of
updating. There are at least two reasons for these flaps. The first
one is packet reordering, where a pre-update RTP or RTCP packet with
an SDES item is delivered to the receiver after the first RTP/RTCP
packet with the updated value. The second reason is the different
code-paths for RTP and RTCP in implementations. An update to the
sender's SDES item parameter can take a different time to propagate
to the receiver than the corresponding media data. For example, an
RTCP packet with the SDES item included that may have been generated
prior to the update can still reside in a buffer and be sent
unmodified. The update of the item's value can at the same time
cause RTP packets to be sent including the header extension, prior to
the RTCP packet being sent.

However, most of these issues can be avoided by the receiver
performing some checks before updating the receiver's stored value.
To handle flaps caused by reordering, SDES items received in RTP
packets with the same or a lower extended sequence number than the
last change MUST NOT be applied, i.e., discard items that can be
determined to be older than the current one. For compound RTCP
packets, which will contain a Sender Report (SR) packet (assuming an
active RTP sender), the receiver can use the RTCP SR Timestamp field
to determine at what approximate time it was transmitted. If the
timestamp is earlier than the last received RTP packet with a header
extension carrying an SDES item, and especially if carrying a
previously used value, the SDES item in the RTCP SDES packet can be
ignored. Note that media processing and transmission pacing can
easily cause the RTP header timestamp field as well as the RTCP SR
timestamp field to not match with the actual transmission time.

4.2.7. RTP Header Compression

When robust header compression (ROHC) [RFC5225] is used with RTP, the
RTP header extension [RFC5285] data itself is not part of what is
being compressed and thus does not impact header compression
performance. The extension indicator (X) bit in the RTP header is

however compressed. It is classified as rarely changing, which may
no longer be true for all RTP header extension usage, in turn leading
to lower header compression efficiency.

5. IANA Considerations

This section makes the following requests to IANA:

o Create a new sub-registry reserved for RTCP SDES items with the
   URN sub-space "urn:ietf:params:rtp-hdrext:sdes:" in the RTP
   Compact Header Extensions registry.

o Register the SDES items appropriate for use with the RTP header
   extension defined in this document.

RFC-editor note: Please replace all occurrences of RFCXXXX with the
RFC number this specification receives when published.

5.1. Registration of an SDES Base URN

IANA is requested to register the below entry in the RTP Compact
Header Extensions registry:

Extension URI: urn:ietf:params:rtp-hdrext:sdes
Description: Reserved as base URN for RTCP SDES items that are also
               defined as RTP Compact header extensions.
Contact: Authors of [RFCXXXX]
Reference: [RFCXXXX]

The reason to register a base URN for an SDES sub-space is that the
name represents an RTCP Source Description item, where a
specification is strongly recommended [RFC3550].

5.2. Creation of an SDES Sub-Registry

IANA is requested to create a sub-registry to the RTP Compact Header
Extensions registry, with the same basic requirements, structure and
layout as the RTP Compact Header Extensions registry.

o Registry name: RTP SDES Compact Header Extensions

o Specification: RFCXXXX and RFCs updating RFCXXXX

o Information required: Same as for RTP Header Extensions [RFC5285]
   registry

o Review process: Same as for RTP Header Extensions [RFC5285]
   registry, with the following requirements added to the expert
   review:

   1. Any registration using an Extension URI that starts with
       "urn:ietf:params:rtp-hdrext:sdes:" (Section 5.1) MUST also
       have a registered Source Description item in the "RTP SDES
       item types" registry.

   2. A security and privacy consideration for the SDES item MUST be
       provided with the registration.

   3. Information MUST be provided on why this SDES item requires
       timely delivery, motivating it to be transported in a header
       extension rather than as RTCP only.

o Size and format of entries: Same as for RTP Header Extensions
   [RFC5285] registry.

o Initial assignments: See Section 5.3 below.

5.3. Registration of SDES Item

It is requested that the following SDES item is registered in the
newly formed RTP SDES Compact Header Extensions registry:

```
Extension URI: urn:ietf:params:rtp-hdrext:sdes:cname
Description:    Source Description: Canonical End-Point Identifier
                (SDES CNAME)
Contact:        Authors of [RFCXXXX]
Reference:      [RFCXXXX]
```

6. Security Considerations

Source Description items may contain data that are sensitive from a
security perspective. There are SDES items that are or may be
sensitive from a user privacy perspective, like CNAME, NAME, EMAIL,
PHONE, LOC and H323-CADDR. Some may contain sensitive information,
like NOTE and PRIV, while others may be sensitive from profiling
implementations for vulnerability or other reasons, like TOOL. The
CNAME sensitivity can vary depending on how it is generated and what
persistence it has. A short term CNAME identifier generated using a
random number generator [RFC7022] may have minimal security
implications, while a CNAME of the form user@host has privacy
concerns, and a CNAME generated from a MAC address has long term
tracking potentials.

In RTP sessions where any type of confidentiality protection is
enabled for RTCP, the SDES item header extensions MUST also be
protected. This implies that to provide confidentiality, users of
SRTP need to implement and use encrypted header extensions per
[RFC6904]. SDES items carried as RTP header extensions MUST then use
commensurate strength algorithms and SHOULD use the same
cryptographic primitives (algorithms, modes) as applied to RTCP
packets carrying corresponding SDES items. If the security level is
chosen to be different for an SDES item in RTCP and RTP header
extension, it is important to motivate the exception, and to consider
the security properties as the worst in each aspect for the different
configurations. It is worth noting that the current Secure RTP
(SRTP) [RFC3711] only provides protection for the next trusted RTP/
RTCP hop, which is not necessarily end-to-end.

The general RTP header extension mechanism [RFC5285] does not itself
contain any functionality that is a significant risk for a denial of
service attack, neither from processing nor storage requirements.
The extension for SDES items defined in this document, can
potentially be a risk. The risk depends on the received SDES item
and its content. If the SDES item causes the receiver to perform a
large amount of processing, create significant storage structures, or
emit network traffic, such a risk does exist. The CNAME SDES item in
the RTP header extension is only a minor risk, as reception of a
CNAME item will create an association between the stream carrying the
SDES item and other RTP streams with the same SDES item. This
usually results in time synchronizing the media streams, thus some
additional processing is performed. However, the application's media
quality is likely more affected by an erroneous or changing
association and media synchronization, than the application quality
impact caused by the additional processing.

As the SDES items are used by the RTP based application to establish
relationships between RTP streams or between an RTP stream and
information about the originating participant, there SHOULD be strong
integrity protection and source authentication of the header
extensions. If not, an attacker can modify the SDES item value to
create erroneous relationship bindings in the receiving application.
For information regarding options for securing RTP, see [RFC7201].

7. Acknowledgments

The authors likes to thank the following individuals for feedback and
suggestions: Colin Perkins, Ben Campbell, and Samuel Weiler.

8. References

8.1. Normative References

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
            Requirement Levels", BCP 14, RFC 2119,
            DOI 10.17487/RFC2119, March 1997,
            <http://www.rfc-editor.org/info/rfc2119>.

[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>.

[RFC5285]   Singer, D. and H. Desineni, "A General Mechanism for RTP
            Header Extensions", RFC 5285, DOI 10.17487/RFC5285, July
            2008, <http://www.rfc-editor.org/info/rfc5285>.

[RFC6904]   Lennox, J., "Encryption of Header Extensions in the Secure
            Real-time Transport Protocol (SRTP)", RFC 6904,
            DOI 10.17487/RFC6904, April 2013,
            <http://www.rfc-editor.org/info/rfc6904>.

8.2. Informative References

[I-D.ietf-mmusic-sdp-bundle-negotiation]
            Holmberg, C., Alvestrand, H., and C. Jennings,
            "Negotiating Media Multiplexing Using the Session
            Description Protocol (SDP)", draft-ietf-mmusic-sdp-bundle-
            negotiation-30 (work in progress), June 2016.

[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>.

[RFC3629]   Yergeau, F., "UTF-8, a transformation format of ISO
            10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November
            2003, <http://www.rfc-editor.org/info/rfc3629>.

[RFC3711]   Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K.
            Norrman, "The Secure Real-time Transport Protocol (SRTP)",
            RFC 3711, DOI 10.17487/RFC3711, March 2004,
            <http://www.rfc-editor.org/info/rfc3711>.

[RFC4566]   Handley, M., Jacobson, V., and C. Perkins, "SDP: Session
            Description Protocol", RFC 4566, DOI 10.17487/RFC4566,
            July 2006, <http://www.rfc-editor.org/info/rfc4566>.

   [RFC4585] Ott, J., Wenger, S., Sato, N., Burmeister, C., and J. Rey,
              "Extended RTP Profile for Real-time Transport Control
              Protocol (RTCP)-Based Feedback (RTP/AVPF)", RFC 4585,
              DOI 10.17487/RFC4585, July 2006,
              <http://www.rfc-editor.org/info/rfc4585>.

   [RFC4588] Rey, J., Leon, D., Miyazaki, A., Varsa, V., and R.
              Hakenberg, "RTP Retransmission Payload Format", RFC 4588,
              DOI 10.17487/RFC4588, July 2006,
              <http://www.rfc-editor.org/info/rfc4588>.

   [RFC5109] Li, A., Ed., "RTP Payload Format for Generic Forward Error
              Correction", RFC 5109, DOI 10.17487/RFC5109, December
              2007, <http://www.rfc-editor.org/info/rfc5109>.

   [RFC5225] Pelletier, G. and K. Sandlund, "RObust Header Compression
              Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP and
              UDP-Lite", RFC 5225, DOI 10.17487/RFC5225, April 2008,
              <http://www.rfc-editor.org/info/rfc5225>.

   [RFC5576] Lennox, J., Ott, J., and T. Schierl, "Source-Specific
              Media Attributes in the Session Description Protocol
              (SDP)", RFC 5576, DOI 10.17487/RFC5576, June 2009,
              <http://www.rfc-editor.org/info/rfc5576>.

   [RFC5888] Camarillo, G. and H. Schulzrinne, "The Session Description
              Protocol (SDP) Grouping Framework", RFC 5888,
              DOI 10.17487/RFC5888, June 2010,
              <http://www.rfc-editor.org/info/rfc5888>.

   [RFC6051] Perkins, C. and T. Schierl, "Rapid Synchronisation of RTP
              Flows", RFC 6051, DOI 10.17487/RFC6051, November 2010,
              <http://www.rfc-editor.org/info/rfc6051>.

   [RFC7022] Begen, A., Perkins, C., Wing, D., and E. Rescorla,
              "Guidelines for Choosing RTP Control Protocol (RTCP)
              Canonical Names (CNAMEs)", RFC 7022, DOI 10.17487/RFC7022,
              September 2013, <http://www.rfc-editor.org/info/rfc7022>.

   [RFC7201] Westerlund, M. and C. Perkins, "Options for Securing RTP
              Sessions", RFC 7201, DOI 10.17487/RFC7201, April 2014,
              <http://www.rfc-editor.org/info/rfc7201>.

   [RFC7656] Lennox, J., Gross, K., Nandakumar, S., Salgueiro, G., and
              B. Burman, Ed., "A Taxonomy of Semantics and Mechanisms
              for Real-Time Transport Protocol (RTP) Sources", RFC 7656,
              DOI 10.17487/RFC7656, November 2015,
              <http://www.rfc-editor.org/info/rfc7656>.

Authors' Addresses

    Magnus Westerlund
    Ericsson
    Farogatan 6
    SE-164 80 Stockholm
    Sweden

    Phone: +46 10 714 82 87
    Email: magnus.westerlund@ericsson.com

    Bo Burman
    Ericsson
    Gronlandsgatan 31
    Stockholm 16480
    Sweden

    Email: bo.burman@ericsson.com

    Roni Even
    Huawei Technologies
    Tel Aviv
    Israel

    Email: roni.even@mail01.huawei.com

    Mo Zanaty
    Cisco Systems
    7100 Kit Creek
    RTP, NC 27709
    USA

    Email: mzanaty@cisco.com