              Methods to Convey Forward Error Correction (FEC)
                    Framework Configuration Information

Abstract

   The Forward Error Correction (FEC) Framework document (RFC 6363)
   defines the FEC Framework Configuration Information necessary for the
   FEC Framework operation. This document describes how to use
   signaling protocols such as the Session Announcement Protocol (SAP),
   the Session Initiation Protocol (SIP), the Real Time Streaming
   Protocol (RTSP), etc. for determining and communicating the
   configuration information between sender(s) and receiver(s).

   This document doesn't define any new signaling protocol.

Copyright Notice

Table of Contents

1. Introduction

   The FEC Framework document [RFC6363] defines the FEC Framework
   Configuration Information that governs the overall FEC Framework
   operation common to any FEC scheme. This information must be
   available at both the sender and receiver(s).

   This document describes how various signaling protocols such as the
   Session Announcement Protocol (SAP) [RFC2974], the Session Initiation
   Protocol (SIP) [RFC3261], the Real Time Streaming Protocol (RTSP)
   [RFC2326], etc. could be used by the FEC scheme (and/or the Content
   Delivery Protocol (CDP)) to communicate the configuration information

between the sender and receiver(s). The configuration information
may be encoded in any compatible format, such as the Session
Description Protocol (SDP) [RFC4566], XML, etc., though this document
refers to SDP encoding usage quite extensively.

   Note that this document doesn't define any new signaling protocol;
   rather, it just provides examples of how existing protocols should
   be used. Also, the list of signaling protocols for unicast is not
   intended to be a complete list.

This document doesn't describe any FEC-Scheme-Specific Information
(FSSI) (for example, how source blocks are constructed) or any
sender- or receiver-side operation for a particular FEC scheme (for
example, whether the receiver makes use of one or more repair flows
that are received). Such FEC scheme specifics should be covered in
separate document(s). This document doesn't mandate a particular
encoding format for the configuration information either.

This document is structured as follows: Section 3 describes the terms
used in this document, Section 4 describes the FEC Framework
Configuration Information, Section 5 describes how to use signaling
protocols for multicast and unicast applications, and Section 6
discusses security considerations.

2. Specification 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 [RFC2119].

3. Terminology/Abbreviations

   This document makes use of the terms/abbreviations defined in the FEC
   Framework document [RFC6363] and defines the following additional
   terms:

   o Media Sender - Node providing original media flow(s) to the 'FEC
      Sender'

   o Media Receiver - Node performing the media decoding

   o FEC Sender - Node performing the FEC encoding on the original
      media flow(s) to produce the FEC repair flow(s)

   o FEC Receiver - Node performing the FEC decoding, as needed, and
      providing the original media flow(s) to the Media Receiver

   o Sender - Same as FEC Sender

   o Receiver - Same as FEC Receiver

   o (Media) Flow - A single media instance, i.e., an audio stream or a
      video stream

   This document deliberately refers to the 'FEC Sender' and 'FEC
   Receiver' as the 'Sender' and 'Receiver', respectively.

4. FEC Framework Configuration Information

   The FEC Framework [RFC6363] defines a minimum set of information that
   is communicated between the sender and receiver(s) for a proper
   operation of an FEC scheme. This information is referred to as "FEC
   Framework Configuration Information". This is the information that
   the FEC Framework needs in order to apply FEC protection to the
   transport flows.

   A single instance of the FEC Framework provides FEC protection for
   all packets of a specified set of source packet flows, by means of
   one or more packet flows consisting of repair packets. As per
   Section 5.5 of the FEC Framework document [RFC6363], the FEC
   Framework Configuration Information includes the following for each
   FEC Framework instance:

   1. Identification of the repair flow(s)

   2. Identification of source flow(s)

   3. Identification of FEC scheme

   4. Length of Explicit Source FEC Payload ID

   5. FSSI

   FSSI basically provides an opaque container to encode FEC-scheme-
   specific configuration information such as buffer size, decoding
   wait-time, etc. Please refer to the FEC Framework document [RFC6363]
   for more details.

   The usage of signaling protocols described in this document requires
   that the application layer responsible for the FEC Framework instance
   provide the value for each of the configuration information
   parameters (listed above) encoded as per the chosen encoding format.
   In case of failure to receive the complete information, the signaling
   protocol module must return an error for Operations, Administration,
   and Maintenance (OAM) purposes and optionally convey this error to
   the application layer. Please refer to Figure 1 of the FEC Framework
   document [RFC6363] for further illustration.

   This document does not make any assumption that the 'FEC Sender' and
   'Media Sender' functionalities are implemented on the same device,
   though that may be the case. Similarly, this document does not make
   any assumption that 'FEC Receiver' and 'Media Receiver'
   functionalities are implemented on the same device, though that may
   be the case. There may also be more than one Media Sender.

4.1. Encoding Format

   The FEC Framework Configuration Information (listed above in
   Section 4) may be encoded in any format, such as SDP, XML, etc., as
   chosen or preferred by a particular FEC Framework instance. The
   selection of such encoding formats or syntax is independent of the
   signaling protocol and beyond the scope of this document.

   Any encoding format that is selected for a particular FEC Framework
   instance must be known to the signaling protocol. This is to provide
   a means (e.g., a field such as Payload Type) in the signaling
   protocol message(s) to convey the chosen encoding format for the
   configuration information so that the payload (i.e., configuration
   information) can be correctly parsed as per the semantics of the
   chosen encoding format at the receiver. Please note that the
   encoding format is not a negotiated parameter, but rather a property
   of a particular FEC Framework instance and/or its implementation.

   Additionally, the encoding format for each FEC Framework
   configuration parameter must be defined in terms of a sequence of
   octets that can be embedded within the payload of the signaling
   protocol message(s). The length of the encoding format must either
   be fixed or be derived by examining the encoded octets themselves.
   For example, the initial octets may include some kind of length
   indication.

   Independent of the encoding formats supported by an FEC scheme, each
   instance of the FEC Framework must use a single encoding format to
   describe all of the configuration information associated with that
   instance. The signaling protocol specified in this document should
   not validate the encoded information, though it may validate the
   syntax or length of the encoded information.

   The reader may refer to the SDP elements document [RFC6364], which
   describes the usage of the 'SDP' encoding format as an example
   encoding format for the FEC Framework Configuration Information.

5. Signaling Protocol Usage

   The FEC Framework [RFC6363] requires that certain FEC Framework
   Configuration Information be available to both the sender and
   receiver(s). This configuration information is almost always
   formulated at the sender (or on behalf of the sender) and somehow
   made available at the receiver(s). While one may envision a static
   method to populate the configuration information at both the sender
   and receiver(s), it would not be optimal, since it would (a) require
   the knowledge of every receiver in advance, (b) require the time and
   means to configure each receiver and sender, and (c) increase the
   possibility of misconfiguration. Hence, there is a benefit in using
   a dynamic method (i.e., signaling protocol) to convey the
   configuration information between the sender and one or more
   receivers.

   Since the configuration information may be needed at a particular
   receiver versus many receivers (depending on the multimedia stream
   being unicast (e.g., Video on Demand (VoD); or multicast, e.g.,
   broadcast or IPTV), we need two types of signaling protocols -- one
   to deliver the configuration information to many receivers via
   multicasting (as described in Section 5.1), and the other to deliver
   the configuration information to one and only one receiver via
   unicasting (as described in Section 5.2).

   Figure 1 below illustrates a sample topology showing the FEC Sender
   and FEC Receiver (which may or may not be the Media Sender and Media
   Receiver, respectively) such that FEC_Sender1 is serving
   FEC_Receiver11, FEC_Receiver12, and FEC_Receiver13 via the multicast
   signaling protocol, whereas FEC_Sender2 is serving only FEC_Receiver2
   via the unicast signaling protocol.

```
        FEC_Sender2---------|         |--------FEC_Receiver2
                            |         |
        FEC_Sender1-------IP/MPLS network
                                  |-----------FEC_Receiver11
                                  |-----------FEC_Receiver12
                                  |-----------FEC_Receiver13
```
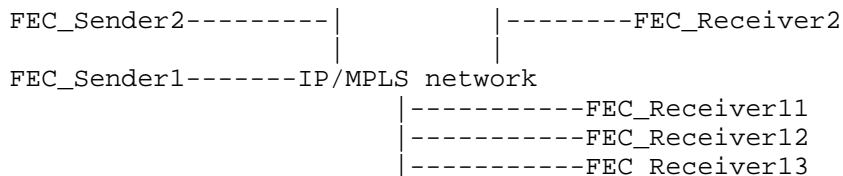
            Figure 1. Topology Using Sender and Receiver

   The rest of the document continues to use the terms 'Sender' and
   'Receiver' to refer to the 'FEC Sender' and 'FEC Receiver',
   respectively.

5.1. Signaling Protocol for Multicasting

   This specification describes using SAP version 2 [RFC2974] as the
   signaling protocol to multicast the configuration information from
   one sender to many receivers. The apparent advantage is that the
   server doesn't need to maintain any state for any receiver using SAP.

      SAP messages are carried over UDP over IP with destination UDP
      port 9875, as described in [RFC2974], and a source UDP port of any
      available number. The SAP message(s) MUST contain an
      authentication header using Pretty Good Privacy (PGP)
      authentication.

   At the high level, a sender, acting as the SAP announcer, signals the
   FEC Framework Configuration Information for each FEC Framework
   instance available at the sender, using the SAP message(s). The
   configuration information, encoded in a suitable format as per
   Section 4.1, is carried in the payload of the SAP message(s). A
   receiver, acting as the SAP listener, listens on a well-known UDP
   port and at least one well-known multicast group IP address (as
   explained in Section 5.1.1). This enables the receiver to receive
   the SAP message(s) and obtain the FEC Framework Configuration
   Information for each FEC Framework instance.

   Using the configuration information, the receiver becomes aware of
   available FEC protection options, corresponding multicast trees (S,G
   or *,G addresses), etc. The receiver may subsequently subscribe to
   one or more multicast trees to receive the FEC streams using out-of-
   band multicasting techniques such as PIM [RFC4601]. This, however,
   is outside the scope of this document.

   Figure 2 below (reprinted from [RFC2974]) illustrates the SAP packet
   format.

```
      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
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     | V=1 |A|R|T|E|C|   auth len    |         msg id hash           |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                                                               |
     :              originating source (32 or 128 bits)             :
     :                                                               :
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                  optional authentication data                 |
     :                          ....                                 :
     *-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
     |                    optional payload type                      |
     +                                        +-+- - - - - - - - - -+
     |                                        |0|                    |
     + - - - - - - - - - - - - - - - - - - - -+-+                    |
     |                                                               |
     :                          payload                              :
     |                                                               |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
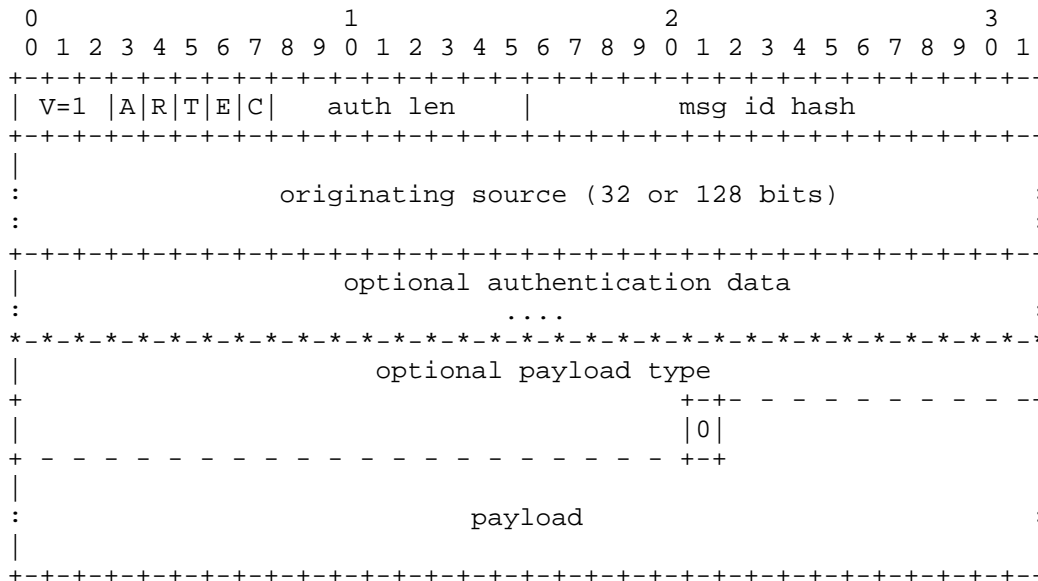
                       Figure 2. SAP Message Format

   While [RFC2974] includes explanations for each field, it is worth
   discussing the 'Payload' and 'Payload Type' fields. The 'Payload'
   field is used to carry the FEC Framework Configuration Information.
   Subsequently, the optional 'Payload Type' field, which is a MIME
   content type specifier, is used to describe the encoding format used
   to encode the payload.

      For example, the 'Payload Type' field may be application/sdp if
      the FEC Framework Configuration Information is encoded in SDP
      format and carried in the SAP payload. Similarly, it would be
      application/xml if the FEC Framework Configuration Information
      were encoded in XML format.

   Section 5.1.1 describes the sender procedure, whereas Section 5.1.2
   describes the receiver procedure in the context of config signaling
   using [RFC2974].

5.1.1. Sender Procedure

   The sender signals the FEC Framework Configuration Information for
   each FEC Framework instance in a periodic SAP announcement message
   [RFC2974]. The SAP announcement message is sent to a well-known
   multicast IP address and UDP port, as specified in [RFC2974]. The
   announcement is multicast with the same scope as the session being
   announced.

   The SAP module at the sender obtains the FEC Framework Configuration
   Information per instance from the 'FEC Framework' module and places
   that in the SAP payload accordingly. A single SAP (announcement)
   message must carry the FEC Framework Configuration Information for a
   single FEC Framework instance. The SAP message is then sent over UDP
   over IP.

      While it is possible to aggregate multiple SAP (announcement)
      messages in a single UDP datagram as long as the resulting UDP
      datagram length is less than the IP MTU of the outgoing interface,
      this specification does not recommend it, since there is no length
      field in the SAP header to identify a SAP message boundary.
      Hence, this specification recommends that a single SAP
      announcement message be sent in a UDP datagram.

   The IP packet carrying the SAP message must be sent to a destination
   IP address of one of the following, depending on the selected scope:

   - 224.2.127.254 (if IPv4 global scope 224.0.1.0-238.255.255.255 is
     selected for the FEC stream), or

   - ff0x:0:0:0:0:0:2:7ffe (if IPv6 multicasting is selected for the FEC
     stream, where x is the 4-bit scope value), or

   - the highest multicast address (239.255.255.255, for example) in the
     relevant administrative scope zone (if IPv4 administrative scope
     239.0.0.0-239.255.255.255 is selected for the FEC stream)

   As defined in [RFC2974], the IP packet carrying a SAP message must
   use destination UDP port 9875 and a source UDP port of any available
   number. The default IP Time to Live (TTL) value (or Hop Limit value)
   should be 255 at the sender, though the sender implementation may
   allow it to be any other value to implicitly create the multicast
   boundary for SAP announcements. The IP Differentiated Services Code
   Point (DSCP) field may be set to any value that indicates a desired
   QoS treatment in the IP network.

The IP packet carrying the SAP message must be sent with a source IP address that is reachable by the receiver. The sender may assign the same IP address in the 'originating source' field of the SAP message as that used in the source IP address of the IP packet.

Furthermore, the FEC Framework Configuration Information must not include any of the reserved multicast group IP addresses for the FEC streams (i.e., source or repair flows), though it may use the same IP address as the 'originating source' address to identify the FEC streams (i.e., source or repair flows). Please refer to IANA assignments for multicast addresses.

The sender must periodically send the 'SAP announcement' message to ensure that the receiver doesn't purge the cached entry or entries from the database and doesn't trigger the deletion of the FEC Framework Configuration Information.

While the time interval between repetitions of an announcement can be calculated as per the very sophisticated but complex method explained in [RFC2974], this document recommends a simpler method in which the user specifies the time interval in the range of 1-200 seconds, with a suggested default value of 60 seconds. In this method, the 'time interval' may be signaled in the SAP message payload, e.g., within the FEC Framework Configuration Information.

   Note that SAP doesn't allow the time interval to be signaled in
   the SAP header. Hence, the usage of a simpler method requires
   that the time interval be included in the FEC Framework
   Configuration Information if the default time interval (60
   seconds) for SAP message repetitions is not used. For example,
   the usage of the 'r=' (repeat time) field in SDP may convey the
   time interval value if the SDP encoding format is used.

The time interval must be chosen to ensure that SAP announcement messages are sent out before the corresponding multicast routing entry, e.g., (S,G) or (*,G) (corresponding to the SAP multicast tree(s)) on the router(s) times out. (It is worth noting that the default timeout period for the multicast routing entry is 210 seconds, per the PIM specification [RFC4601], though the timeout period may be set to another value as allowed by the router implementation.)

   A SAP implementation may also support the complex method for
   determining the SAP announcement time interval and provide the
   option to select it.

The sender may choose to delete the announced FEC Framework
Configuration Information, as defined in Section 4 of [RFC2974]. The
explicit deletion is useful if the sender no longer desires to send
any more FEC streams.

If the sender needs to modify the announced FEC Framework
Configuration Information for one or more FEC instances, then the
sender must send a new announcement message with a different 'Message
Identifier Hash' value as per the rules described in Section 5 of
RFC 2974 [RFC2974]. Such an announcement message should be sent
immediately (without having to wait for the time interval) to ensure
that the modifications are received by the receiver as soon as
possible. The sender must also send the SAP deletion message to
delete the previous SAP announcement message (i.e., with the previous
'Message Identifier Hash' value).

5.1.2. Receiver Procedure

The receiver must listen on UDP port 9875 for packets arriving with
an IP destination address of either 224.2.127.254 (if an IPv4 global
scope session is used for the FEC stream), ff0x:0:0:0:0:0:2:7ffe (if
IPv6 is selected, where x is the 4-bit scope value), or the highest
IP address (239.255.255.255, for example) in the relevant
administrative scope zone (if IPv4 administrative scope 239.0.0.0-
239.255.255.255 is selected for the FEC stream). These IP addresses
are mandated for SAP usage by RFC 2974 [RFC2974].

The receiver, upon receiving a SAP announcement message, creates an
entry, if it doesn't already exist, in a local database and passes
the FEC Framework Configuration Information from the SAP Payload
field to the 'FEC Framework' module. Each entry also maintains a
timeout value, which is (re)set to five times the time interval
value, which in turn is either the default of 60 seconds or the value
signaled by the sender.

    Note that SAP doesn't allow the time interval to be signaled in
    the SAP header. Hence, the time interval should be included in
    the FEC Framework Configuration Information -- for example, the
    usage of the 'r=' (repeat time) field in SDP to convey the time
    interval value if the SDP encoding format is used.

The timeout value associated with each entry is reset when the
corresponding announcement (please see Section 5 of [RFC2974]) is
received. If the timeout value for any entry reaches zero, then that
entry must be deleted from the database, as described in Section 4 of
[RFC2974]. The receiver, upon receiving a SAP delete message, must
delete the matching SAP entry in its database, as described in
Section 4 of [RFC2974].

The deletion of a SAP entry must result in the receiver no longer
using the relevant FEC Framework Configuration Information for the
corresponding instance and no longer subscribing to any related FEC
streams.

5.2. Signaling Protocol for Unicasting

This document describes leveraging any signaling protocol that is
already used by the unicast application, for exchanging the FEC
Framework Configuration Information between two nodes.

For example, a multimedia (VoD) client may send a request via
unicasting for a particular content to the multimedia (VoD) server,
which may offer various options such as encodings, bitrates,
transport, etc. for the content. The client selects the suitable
options and answers the server, paving the way for the content to be
unicast on the chosen transport from the server to the client. This
offer/answer signaling, described in [RFC3264], is commonly utilized
by many application protocols, such as SIP, RTSP, etc.

The fact that two nodes desiring unicast communication almost always
rely on an application to first exchange the application-related
parameters via the signaling protocol makes it logical to enhance
such signaling protocol(s) to (a) convey the desire for the FEC
protection and (b) subsequently also exchange FEC parameters, i.e.,
the FEC Framework Configuration Information. This enables the node
acting as the offerer to offer 'FEC Framework Configuration
Information' for each available FEC instance and the node acting as
the answerer to convey the chosen FEC Framework instance(s) to the
offerer. The usage of the FEC Framework instance is explained in the
FEC Framework document [RFC6363].

While enhancing an application's signaling protocol to exchange FEC
parameters is one method (briefly explained above), an alternative
method would be to have a unicast-based generic protocol that could
be used by two nodes, independent of the application's signaling
protocol. The latter is not covered by this document, of course.

The remainder of this section provides example signaling protocols
and explains how they can be used to exchange the FEC Framework
Configuration Information.

5.2.1. SIP

SIP [RFC3261] is an application-level signaling protocol to create,
modify, and terminate multimedia sessions with one or more
participants. SIP also enables the participants to discover one
another and to agree on a characterization of a multimedia session

they would like to share. SIP runs on either TCP, UDP, or Stream
Control Transmission Protocol (SCTP) transport and uses SDP as the
encoding format to describe multimedia session attributes.

SIP already uses an offer/answer model with SDP as described in
[RFC3264] to exchange information between two nodes to establish
unicast sessions between them. This document extends the usage of
this model for exchanging the FEC Framework Configuration Information
(described in Section 4). Any SDP-specific enhancements to
accommodate the FEC Framework are covered in the SDP elements
specification [RFC6364].

5.2.2. RTSP

RTSP [RFC2326] is an application-level signaling protocol for control
over the delivery of data with real-time properties. RTSP provides
an extensible framework to enable controlled, on-demand delivery of
real-time data such as audio and video. RTSP runs on either TCP or
UDP transports.

RTSP already provides an ability to extend the existing method with
new parameters. This specification defines the
'FEC-protection-needed' option tag (please see Section 7 for IANA
Considerations) and prescribes including it in the Require (or
Proxy-Require) header of SETUP (method) request messages, so as to
request FEC protection for the data.

The node receiving such a request either responds with a '200 OK'
message that includes offers, i.e., available FEC options (e.g., FEC
Framework Configuration Information for each instance) or a '551
Option not supported' message. A sample of a related message
exchange is shown below.

    Node1->Node2: SETUP < ... > RTSP/1.0
                   CSeq: 1
                   Transport: <omitted for simplicity>
                   Require: FEC-protection-needed

    Node2->Node1: RTSP/1.0 200 OK
                   CSeq: 1
                   Transport: <omitted for simplicity>

The requesting node (Node1) may then send a new SETUP message to
convey the selected FEC protection to Node2 and proceed with regular
RTSP messaging.

Suffice it to say that if the requesting node (Node1) received a '551
Option not supported' response from Node2, then the requesting node
(Node1) may send the SETUP message without using the Require header.

6. Security Considerations

This document recommends that SAP message(s) be authenticated to
ensure sender authentication, as described in Section 5.1.

There are no additional security considerations other than those
already covered in [RFC2974] for SAP, [RFC2326] for RTSP, and
[RFC3261] for SIP.

7. IANA Considerations

IANA has registered a new RTSP option tag (option-tag), listed below,
in the RTSP/1.0 Option Tags table of the "Real Time Streaming
Protocol (RTSP)/1.0 Parameters" registry available from
http://www.iana.org/, and it provides the following information in
compliance with Section 3.8.1 of [RFC2326]:

   o Name of option-tag: FEC-protection-needed

   o Description: See Section 5.2.2

   o Change Control: IETF

8. Acknowledgments

Thanks to Colin Perkins for pointing out the issue with the time
interval for the SAP messages. Additionally, thanks to Vincent Roca,
Ali Begen, Mark Watson, Ulas Kozat, and David Harrington for greatly
improving this document.

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.

   [RFC2974]   Handley, M., Perkins, C., and E. Whelan, "Session
               Announcement Protocol", RFC 2974, October 2000.

   [RFC6363]   Watson, M., Begen, A., and V. Roca, "Forward Error
               Correction (FEC) Framework", RFC 6363, October 2011.

   [RFC6364]   Begen, A., "Session Description Protocol Elements for the
               Forward Error Correction (FEC) Framework", RFC 6364,
               October 2011.

9.2. Informative References

   [RFC2326]   Schulzrinne, H., Rao, A., and R. Lanphier, "Real Time
               Streaming Protocol (RTSP)", RFC 2326, April 1998.

   [RFC3261]   Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston,
               A., Peterson, J., Sparks, R., Handley, M., and E.
               Schooler, "SIP: Session Initiation Protocol", RFC 3261,
               June 2002.

   [RFC3264]   Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model
               with Session Description Protocol (SDP)", RFC 3264,
               June 2002.

   [RFC4566]   Handley, M., Jacobson, V., and C. Perkins, "SDP: Session
               Description Protocol", RFC 4566, July 2006.

   [RFC4601]   Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas,
               "Protocol Independent Multicast - Sparse Mode (PIM-SM):
               Protocol Specification (Revised)", RFC 4601, August 2006.

Author's Address

   Rajiv Asati
   Cisco Systems
   7025-6 Kit Creek Rd.
   RTP, NC 27709-4987

   EMail: rajiva@cisco.com