           Methods to convey FEC Framework Configuration Information
                draft-ietf-fecframe-config-signaling-04.txt

Abstract

   FEC Framework document [FECARCH] defines the FEC Framework
   Configuration Information necessary for the FEC framework operation.
   This document describes how to use existing signaling protocols to
   determine and dynamically communicate the Configuration information
   between sender(s) and receiver(s).

The list of current Internet-Drafts can be accessed at
     http://www.ietf.org/ietf/1id-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 July 11, 2011.

Copyright Notice

Table of Contents

1. Introduction

FEC Framework document [FECARCH] 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 sender and reciever(s).

This document describes how to use various signaling protocols to
communicate the Configuration information between sender and
receiver(s). The configuration information may be encoded in any
compatible format such as SDP [RFC4566], XML etc. A signaling
protocol could be utilised by any FEC scheme and/or any Content
Delivery Protocol (CDP).

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 such that Section 2 describes the terms
used in this document, section 3 describes the FEC Framework
Configuration Information, section 4 describes how to use signaling
protocol for the multicast and unicast applications, and section 5
describes security consideration.

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 [FECARCH] 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 [FECARCH] defines a minimum set of information
that MUST be 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 the

FEC Framework document [FECARCH] section 6.5, 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. FEC Scheme Specific Information (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 [FECARCH]
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
parameter (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 the Operation,
Administration and Maintenance (OAM) purposes and optionally convey
to the application layer. Please refer to the figure 1 of the FEC
Framework document [FECARCH] 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 Senders.

4.1. Encoding Format

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

   Whatever encoding format is selected for a particular FEC framework
   instance, it 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 derived by examining the encoded octets themselves.
   For example, the initial octets may include some kind of length
   indication.

   Independent of what all 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 [FECSDP], which
   describes the usage of 'SDP' encoding format as an example encoding
   format for FEC Framework Configuration Information.

5. Signaling Protocol Usage

   FEC Framework [FECARCH] requires certain FEC Framework Configuration
   Information to be available to both sender and receiver(s). This
   configuration information is almost always formulated at the sender
   (or on behalf of a sender), and somehow made available at the
   receiver(s). While one may envision a static method to populate the
   configuration information at both sender and receiver(s), it would

not be optimal since it would (i) require the knowledge of every
receiver in advance, (b) require the time and means to configure
each receiver and sender, and (c) increase the misconfiguration
possibility. Hence, there is a benefit in using a dynamic method
i.e., signaling protocol to convey the configuration information
between 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, 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
(described in section 4.1), and the other to deliver the
configuration information to one and only one receiver via
unicasting (described in section 4.2).

Figure 1 below illustrates a sample topology showing the FEC sender
and FEC receiver (that may or may not be the Media Sender and Media
Receiver respectively) such that FEC_Sender1 is serving
FEC_Receiver11,12,13 via the multicast signaling protocol, whereas
the 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
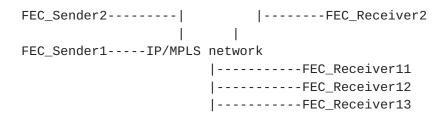

The rest of the section continues to use the terms 'Sender' and
'Receiver' to refer to the 'FEC Sender' and 'FEC Receiver'
respectively.

5.1. Signaling Protocol for Multicasting

This specification describes using Session Announcement Protocol
(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.

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 the section 3.1, 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 the section 4.1.1). This enables the receiver to receive the SAP message(s) and obtains the FEC Framework Configuration Information for each FEC Framework Instance.

One may refer to 'Requirements for IP Multicast Session Announcement in the Internet' document [SAP-REQ] to know about the SAP limitations.

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.

SAP message is carried over UDP over IP. The destination UDP port MUST be 9875 and source UDP port may be any available number. The SAP message(s) SHOULD contain an authentication header and MAY employ cryptography. One cryptography method suggested by this specification is the usage of Group Cryptography as specified in GDOI [RFC3547].

Figure 2 below illustrates the SAP packet format (it is reprinted from the RFC2974) -

```
   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                              :
  |                                                               |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
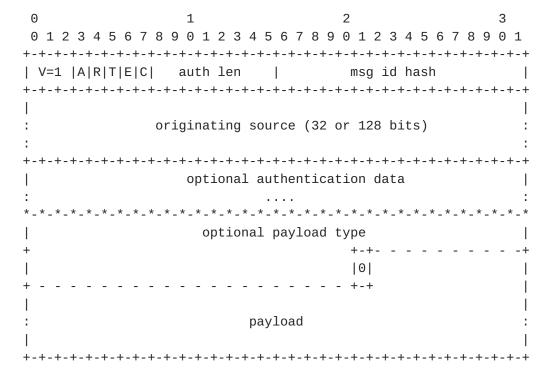
                   Figure 2 SAP Message format

   While the RFC2974 includes explanation for each field, it is worth
   discussing the 'Payload' and 'Payload Type' fields. The 'Payload'
   field MUST be used to carry the FEC Framework Configuration
   Information. Subsequently, the optional 'Payload Type' field, which
   is a MIME content type specifier, MUST 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 was encoded in XML format.

5.1.1. Sender Procedure

   The sender signals the FEC framework configuration 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 SAP message boundary. Hence,
   this specification recommends single SAP announcement message to
   be sent in a UDP datagram.

The IP packet carrying the SAP message MUST be sent to 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)

The destination UDP port MUST be 9875 and source UDP port may be any
available number. The default IP TTL value (or Hop Limit value)
SHOULD be 255, though the implementation may allow it to be any
other value to implicitly create the multicast boundary for SAP
announcements. The IP 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 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 the one 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(s) from the database and doesn't trigger the deletion of FEC Framework Configuration Information.

   Please note that the deletion of FEC Framework Configuration
   Information SHOULD NOT mean that the receiver stops its FEC
   processing for the instance for which it had already got the
   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], the preferred and simpler method recommended by this specification is to let the user specify the time interval from the range of 1-200 seconds with suggested default being 60 seconds. 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 times out. (It is worth noting that the default time-out period for the multicast routing entry is 210 seconds, per the PIM specification [RFC4601], though the time-out period may be set to another value as allowed by the router implementation.)

   The SAP implementation MAY also support the complex method for
   determining the SAP announcement time interval, and provide the
   option to select it over the simpler method.

When simpler method is used, 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 simpler method desires the
   time-interval to be included in the FEC Framework Configuration
   Information, if the default time interval (=60 seconds) for SAP
   message repeations is not deemed enough. For example, the usage of
   "r=" (repeat time) field in SDP to convey the time-interval value,
   if SDP encoding format is used.

The sender may choose to delete the announced FEC Framework Configuration Information by sending a 'SAP deletion' message. This deletion may be useful if the sender no longer desires to send anymore 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 RFC2974 [RFC2974]. Such 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
IP destination address of either 224.2.127.254 (if IPv4 global scope
session is used for the FEC stream), or 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 RFC2974 [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
time-out value, which is (re)set to the five times the time-interval
value, which is either the default = 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
  "r=" (repeat time) field in SDP to convey the time-interval value,
  if SDP encoding format is used.

The time-out value associated with each entry is reset when the
corresponding annoucement (please see section 5 of [RFC2974]) is
received. If the time-out value for any entry reaches zero, then the
entry is deleted from the database.

The receiver, upon receiving a SAP delete message, MUST delete the
matching SAP entry in its database. This SHOULD result in the
receiver no longer using the relevant FEC Framework Configuration
Information for the corresponding instance, and SHOULD no longer
subscribe 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 to the server, paving the way for the content to
   be unicast on the chosen transport from 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, it is 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.,
   FEC Framework Configuration Information. This enables the node
   acting as the offerer to offer 'FEC Framework Configuration
   Information' for each of available FEC instances, and the node
   acting as the answerer conveying the chosen FEC Framework
   instance(s) to the offerer. The usage of FEC framework instance is
   explained the FEC Framework document [FECARCH].

   While enhancing an application's signaling protocol to exchange FEC
   parameters is one method (briefly explained above), another 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 method is under investigation and may be covered by a
   separate document.

   The remainder of this section provides example signaling protocols
   and explains how they can be used to exchange 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 or UDP or SCTP transport, and uses SDP as the encoding format to describe multmedia session attributes.

SIP already uses an offer/answer model with SDP, described in [RFC3264], to exchange the 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, explained in section 3. Any SDP specific enhancements to accommodate the FEC Framework are covered in the SDP Elements specification [FECSDP].

5.2.2. RSTP

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 'FEC Protection Required' option-tag (please see section 6 for IANA Considerations) and prescribes including it in the Require (or Proxy-Require) header of SETUP (method) request message, so as to request for FEC protection for the data.

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

```
Node1->Node2:  SETUP < ... > RTSP/1.0
               CSeq: 1
               Transport: <omitted for simplicity>
               Require: FECprotectionRequired

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 to say, if the requesting node (Node1) received '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 SAP message(s) be authenticated to ensure
sender authentication, as described in section 5.

There is no additional security consideration other than what's
already covered in [RFC2974] for SAP, [RFC2326] for RTSP, and
[RFC3261] for SIP.

7. IANA Considerations

This document requests IANA to register a new option-tag for FEC
protection required, as described in section 4.2.2, and provides the
following information in compliance with section 3.8.1 in [RFC2326]:

   . Name of option   = FECprotectionRequired

   . Change of 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 and Ulas Kozat for greatly improving this
document.

This document was prepared using 2-Word-v2.0.template.dot.

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.

[FECARCH] Watson, M., "Forward Error Correction (FEC) Framework",
          draft-ietf-fecframe-framework-10 (work in progress), May
          2011.

[FECSDP] Begen, A., "SDP Elements for FEC Framework", draft-ietf-
          fecframe-sdp-elements-11 (work in progress), April 2011.

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

9.2. Informative References

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

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

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

[RFC3261] Handley, M., Schulzrinne, H., Schooler, E. and J.
          Rosenberg, "SIP: Session Initiation Protocol", RFC 3261,
          June 2002.

[RFC4601] Fenner, etc., "Protocol Independent Multicast - Sparse
          Mode (PIM-SM): Protocol Specification", RFC 4601, August
          2006.

[RFC3547] Baugher, etc., "The Group Domain of Interpretation", RFC
          3547, July 2003.

[SAP-REQ] Asaeda, etc., "Requirements for IP Multicast Session
          Announcement in the Internet, draft-ietf-mboned-session-
          announcement-req-03, September 2010.

Author's Addresses

   Rajiv Asati
   Cisco Systems,
   7025-6 Kit Creek Rd, RTP, NC, 27709-4987
   Email: rajiva@cisco.com