Network Working Group
Request for Comments: 4756
Category: Standards Track

A. Li
Hyervision

November 2006

Forward Error Correction Grouping Semantics in Session Description Protocol

Status of This Memo

Copyright Notice

Abstract

This document defines the semantics that allow for grouping of Forward Error Correction (FEC) streams with the protected payload streams in Session Description Protocol (SDP). The semantics defined in this document are to be used with "Grouping of Media Lines in the Session Description Protocol" (RFC 3388) to group together "m" lines in the same session.

Table of Contents

1. Introduction

The media lines in an SDP [3] session may be associated with each other in various ways. SDP itself does not provide methods to convey the relationships between the media lines. Such relationships are indicated by the extension to SDP as defined in "Grouping of Media Lines in the Session Description Protocol" (RFC 3388) [2]. RFC 3388 defines two types of semantics: Lip Synchronization and Flow Identification.

Forward Error Correction (FEC) is a common technique to achieve robust communication in error-prone environments. In this document, we define the semantics that allows for grouping of FEC streams with the protected payload streams in SDP by further extending RFC 3388.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD, "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

3. Forward Error Correction (FEC)

Forward Error Correction (FEC) is a common technique to achieve robust communication in error-prone environments. In FEC, communication uses a bandwidth that is more than payload to send redundantly coded payload information. The receivers can readily recover the original payload even when some communication is lost in the transmission. Compared to other error correction techniques (such as retransmission), FEC can achieve much lower transmission delay, and it does not have the problem of implosion from retransmission requests in various multicast scenarios.

In general, the FEC data can be sent in two different ways: (1) multiplexed together with the original payload stream or (2) as a separate stream. It is thus necessary to define mechanisms to indicate the association relationship between the FEC data and the payload data they protect.

When FEC data are multiplexed with the original payload stream, the association relationship may, for example, be indicated as specified in "An RTP Payload for Redundant Audio Data" (RFC 2198) [4]. The generic RTP payload format for FEC [5] uses that method.

When FEC data are sent as a separate stream from the payload data, the association relationship can be indicated in various ways. This document on the FEC media line grouping specifies a mechanism for indicating such relationships.

4. FEC Grouping

4.1. FEC Group

Each "a=group" line is used to indicate an association relationship between the FEC streams and the payload streams. The streams included in one "a=group" line are called a "FEC Group".

Each FEC group MAY have one or more than one FEC stream, and one or more than one payload stream. For example, it is possible to have one payload stream protected by more than one FEC stream , or multiple payload streams sharing one FEC stream.

Grouping streams in a FEC group only indicates the association relationship between streams. The detailed FEC protection scheme/parameters are conveyed through the mechanism of the particular FEC algorithm used. For example, the FEC grouping is used for generic RTP payload for FEC [5] to indicate the association relationship between the FEC stream and the payload stream. The detailed protection level and length information for the Unequal Loss Protection (ULP) algorithm is communicated in band within the FEC stream.

4.2. Offer / Answer Consideration

The backward compatibility in offer / answer is generally handled as specified in RFC 3388 [2].

Depending on the implementation, a node that does not understand FEC grouping (either does not understand line grouping at all, or just does not understand the FEC semantics) SHOULD respond to an offer containing FEC grouping either (1) with an answer that ignores the grouping attribute or (2) with a refusal to the request (e.g., 488 Not acceptable here or 606 Not acceptable in SIP).

In the first case, the original sender of the offer MUST establish the connection without FEC. In the second case, if the sender of the offer still wishes to establish the session, it SHOULD re-try the request with an offer without FEC.

4.3. Example of FEC Grouping

The following example shows a session description of a multicast conference. The first media stream (mid:1) contains the audio stream. The second media stream (mid:2) contains the Generic FEC [5] protection for the audio stream. These two streams form an FEC group. The relationship between the two streams is indicated by the "a=group:FEC 1 2" line. The FEC stream is sent to the same multicast

group and has the same Time to Live (TTL) as the audio, but on a port number two higher. Likewise, the video stream (mid:3) and its Generic FEC protection stream (mid:4) form another FEC group. The relationship between the two streams is indicated by the "a=group:FEC 3 4" line. The FEC stream is sent to a different multicast address, but has the same port number (30004) as the payload video stream.

```
v=0
o=adam 289083124 289083124 IN IP4 host.example.com
s=ULP FEC Seminar
t=0 0
c=IN IP4 224.2.17.12/127
a=group:FEC 1 2
a=group:FEC 3 4
m=audio 30000 RTP/AVP 0
a=mid:1
m=audio 30002 RTP/AVP 100
a=rtpmap:100 ulpfec/8000
a=mid:2
m=video 30004 RTP/AVP 31
a=mid:3
m=video 30004 RTP/AVP 101
c=IN IP4 224.2.17.13/127
a=rtpmap:101 ulpfec/8000
a=mid:4
```

5. Security Considerations

There is a weak threat for the receiver that the FEC grouping can be modified to indicate FEC relationships that do not exist. Such attacks may result in failure of FEC to protect, and/or mishandling of other media payload streams. It is recommended that the receiver SHOULD do integrity check on SDP and follow the security considerations of SDP [3] to only trust SDP from trusted sources.

6. IANA Considerations

This document defines the semantics to be used with grouping of media lines in SDP as defined in RFC 3388. The semantics defined in this document are to be registered by the IANA when they are published in standards track RFCs.

The following semantics have been registered by IANA in Semantics for the "group" SDP Attribute under SDP Parameters.

Semantics	Token	Reference
Forward Error Correction	FEC	RFC 4756

7. Acknowledgments

The author would like to thank Magnus Westerlund, Colin Perkins, Joerg Ott, and Cullen Jennings for their feedback on this document.

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] Camarillo, G., Eriksson, G., Holler, J., and H. Schulzrinne, "Grouping of Media Lines in the Session Description Protocol (SDP)", RFC 3388, December 2002.

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

8.2. Informative References

[4] Perkins, C., Kouvelas, I., Hodson, O., Hardman, V., Handley, M., Bolot, J., Vega-Garcia, A., and S. Fosse-Parisis, "RTP Payload for Redundant Audio Data", RFC 2198, September 1997.

[5] Li, A., "An RFC Payload Format for Generic FEC", Work in Progress.

Author's Address

Adam H. Li
HyerVision
10194 Wateridge Circle #152
San Diego, CA 92121
U.S.A.

Tel: +1 858 622 9038
EMail: adamli@hyervision.com

Full Copyright Statement

Intellectual Property

Acknowledgement

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