CLUE Protocol Data Channel
draft-ietf-clue-datachannel-02

Abstract

   This document defines how to use the WebRTC Data Channel mechanism,
   together with the Data Channel Establishment Protocol (DCEP) in order
   to establish a data channel, referred to as CLUE Data Channel, for
   transporting CLUE protocol messages between two CLUE entities.

   The document defines the SCTP considerations specific to a CLUE Data
   Channel, the SDP offer/answer procedures for negotiating the
   establishment of, and the DCEP procedures for opening, a CLUE Data
   Channel.

   Details and procedures associated with the CLUE protocol are outside
   the scope of this document.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on April 30, 2015.

Copyright Notice

Table of Contents

1. Introduction

This document defines how to use the WebRTC Data Channel mechanism
[I-D.ietf-rtcweb-data-channel], together with the Data Channel
Establishment Protocol (DCEP) [I-D.ietf-rtcweb-data-protocol] in
order to establish a data channel, referred to as CLUE Data Channel,
for transporting CLUE protocol [I-D.ietf-clue-protocol] messages
between CLUE entities.

The document defines the SCTP considerations specific to a CLUE Data
Channel, the SDP offer/answer [RFC3264] procedures for negotiating
the establishment of, and the DCEP procedures for opening, a CLUE
Data Channel.

Details and procedures associated with the CLUE protocol are outside
the scope of this document.

2. Conventions

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 BCP 14, RFC 2119
[RFC2119].

WebRTC Data Channel refers to a SCTPoDTLS association
[I-D.ietf-tsvwg-sctp-dtls-encaps] that is used to transport non-media
data between two entities, according to the procedures in
[I-D.ietf-rtcweb-data-channel].

CLUE Data Channel refers to a WebRTC Data Channel
[I-D.ietf-rtcweb-data-channel], with a specific set of SCTP
characteristics, and usage of the Data Channel Establishment Protocol
(DCEP) [I-D.ietf-rtcweb-data-protocol] in order to open a WebRTC Data
Channel for the purpose of transporting CLUE protocol
[I-D.ietf-clue-protocol] messages between two CLUE entities.

CLUE entity refers to a SIP User Agent (UA) [RFC3261] that supports
the CLUE Data Channel and the CLUE protocol.

CLUE session refers to a SIP session [RFC3261] between to SIP UAs,
where a CLUE Data Channel, associated with the SIP session, has been
established between the SIP UAs.

[RFC4960] defines an SCTP stream as a unidirectional logical channel
established from one to another associated SCTP endpoint, within
which all user messages are delivered in sequence except for those
submitted to the unordered delivery service.

[RFC4960] defines an SCTP identifier as a unsigned integer, which
identifies a SCTP stream.

3. CLUE Data Channel

3.1. General

This section describes the realization of a CLUE Data Channel. This
includes a set of SCTP characteristics specific to a CLUE Data
Channel, and usage of the Data Channel Establishment Protocol (DCEP)
[I-D.ietf-rtcweb-data-protocol] in order to open a WebRTC Data
Channel for the purpose of transporting CLUE protocol
[I-D.ietf-clue-protocol] messages between two CLUE entities.

As described in [I-D.ietf-rtcweb-data-channel], the SCTP streams
realizing a WebRTC Data Channel must be associated with the same SCTP
association. In addition, both SCTP streams realizing the WebRTC
Data Channel must use the same SCTP stream identifier value. These
rules also apply to a CLUE Data Channel.

Within a given CLUE session, a CLUE entity MUST use a single CLUE
Data Channel for transport of all CLUE messages towards its peer.

3.2. Data Channel Establishment Protocol (DCEP) Usage

A CLUE entity MUST support the Data Channel Establishment Protocol
(DCEP) [I-D.ietf-rtcweb-data-channel], which can be used in order to
open a WebRTC Data Channel.

In the absence of some other mechanism, a CLUE entity MUST use DCEP
in order to open a CLUE Data Channel.

NOTE: This document does not define any other mechanism for opening a
CLUE Data Channel, but such might be defined in future
specifications.

The details of the DCEP usage with a CLUE Data Channel are described
in Section 4.1.

3.3. SCTP Considerations

3.3.1. SCTP Payload Protocol Identifier (PPID)

As described in [I-D.ietf-rtcweb-data-protocol], the PPID value 50 is
used when sending a DCEP message on a WebRTC Data Channel.

A CLUE entity MUST use the PPID value 51 when sending a CLUE message
on a CLUE Data Channel.

NOTE: As described in [I-D.ietf-rtcweb-data-channel], the PPID value 51 indicates that the SCTP message contains data encoded in a UTF-8 format. The PPID value 51 does not indicate what application protocol is transported in a WebRTC Data Channel, only the format in which the data is encoded.

```
                 +----------+------------+
                 | Protocol | PPID Value |
                 +----------+------------+
                 |   DCEP   |     50     |
                 |   CLUE   |     51     |
                 +----------+------------+
```

Table 1: CLUE Data Channel PPID Values

3.3.2. Reliability

The usage of SCTP for the CLUE Data Channel ensures reliable transport of CLUE protocol [I-D.ietf-clue-protocol] messages.

A CLUE entity MUST NOT use the partial reliability and limited retransmission extensions defined in [RFC3758].

NOTE: [I-D.ietf-rtcweb-data-channel] requires the support of the partial reliability extension defined in [RFC3758]. This is not needed for a CLUE Data Channel, as messages are required to always be sent reliably. [I-D.ietf-rtcweb-data-channel] also mandates support of the limited retransmission policy defined in [I-D.ietf-tsvwg-sctp-prpolicies].

3.3.3. Order

A CLUE entity MUST use the ordered delivery SCTP service, as described in section 6.6 of [RFC4960].

3.3.4. Stream Reset

A CLUE entity MUST support the stream reset extension defined in [RFC6525].

The dynamic address reconfiguration extension defined in [RFC5061] MUST be used to signal the support of the stream reset extension defined in [RFC6525]. Other features of [RFC5061] MUST NOT be used.

3.3.5. Interleaving

A CLUE entity SHOULD support the message interleaving mechanism defined in [I-D.ietf-tsvwg-sctp-ndata].

3.3.6. SCTP Multihoming

SCTP multihoming cannot be used for a CLUE Data Channel.

NOTE: SCTPoDTLS does not support SCTP multihoming.

4. CLUE Data Channel Procedures

4.1. Open CLUE Data Channel

Once the SCTP association, to be used to realized the CLUE Data Channel, has been established, the offerer [RFC3264] is responsible for opening the CLUE Data Channel. If DCEP is used, the offerer MUST send a DCEP DATA_CHANNEL_OPEN message [I-D.ietf-rtcweb-data-protocol]. The value of the 'protocol' field MUST be "CLUE". The value of the 'channel type' MUST be 'DATA_CHANNEL_RELIABLE'.

OPEN ISSUE: We need to determine whether we shall include a version number in the 'protocol' field value for CLUE.

NOTE: A new 'protocol' value for CLUE needs to be registered with IANA in the 'Protocol Registry' defined by [I-D.ietf-rtcweb-data-protocol].

Once the offerer has received the associated DCEP DATA_CHANNEL_ACK message [I-D.ietf-rtcweb-data-protocol], the CLUE Data channel has been opened.

If the offerer receives a DCEP DATA_CHANNEL_OPEN message, for the purpose of opening a CLUE Data Channel, the offerer MUST reset the SCTP stream, in order to prevent two CLUE Data Channels from being established within the same CLUE session. The offerer MUST NOT send a DCEP DATA_CHANNEL_ACK message.

4.2. Close CLUE Data Channel

DCEP [I-D.ietf-rtcweb-data-protocol] does not define a message for closing a WebRTC Data Channel. As described in [I-D.ietf-rtcweb-data-protocol], in order to close a CLUE Data Channel, a SCTP reset message is sent, in order to close the SCTP stream associated with the CLUE Data Channel. The SCTP association,

and WebRTC Data Channels associated with other SCTP streams, are not
affected by the SCTP reset message.

Section 5.7 describes how to terminate the SCTP association used for
the CLUE data channel.

4.3. SCTP Association Failure

In case of SCTP association failure, the offerer is responsible for
trying to re-establish the SCTP association (including sending a new
SDP offer, if needed). Once the SCTP association has been
successfully re-established, the offerer is responsible for sending a
DCEP DATA_CHANNEL_OPEN message.

5. SDP Offer/Answer Procedures

5.1. General

This section describes how an SDP media description ("m=") line
describing a SCTPoDTLS association, to be used to realize a CLUE Data
Channel, is created, and how it is used in SDP offers and answers
[RFC3264].

NOTE: The procedures associated with creating an "m=" line describing
media (e.g. audio and video) for a CLUE session are outside the scope
of this document.

OPEN ISSUE (Q1): It is FFS whether the SDP-based WebRTC Data Channel
Negotiation mechanism [I-D.ejzak-mmusic-data-channel-sdpneg] will be
used with the CLUE Data Channel. It depends on whether the draft
will progress in MMUSIC, and whether it will be finalized before the
publication of the CLUE mechanism.

OPEN ISSUE (Q2): As the SDP offer/answer procedures are generic to
SCTPoDTLS association, it is FFS whether we need to specify them, or
whether we can simply refer to draft-ietf-mmusic-sctp-sdp.

5.2. SDP Media Description Fields

The field values of the "m=" line for the SCTPoDTLS association are
set as following:

```
+---------------+-----------------+-------------+-----------------+
|     media     |      port       |    proto    |       fmt       |
+---------------+-----------------+-------------+-----------------+
| "application" | DTLS port value | "DTLS/SCTP" | SCTP port value |
+---------------+-----------------+-------------+-----------------+
```

Table 2: SDP "proto" field values

5.3. SDP sctpmap Attribute

The field values of the SDP sctpmap attribute, associated with the
"m=" line describing the SCTPoDTLS association, are set as following:

```
+---------------------------+----------------------+
|       sctpmap-number      |          app         |
+---------------------------+----------------------+
| fmt value of the "m=" line | "webrtc-datachannel" |
+---------------------------+----------------------+
```

Table 3: SDP "proto" field values

5.4. Generating the Initial Offer

The procedures for the offerer follow the normal procedures defined
in [RFC3264].

When the offerer creates an offer, which contains an "m=" line
describing a SCTPoDTLS association, it assigns the field values to
the "m=" line according to the procedures in Section 5.2. In
addition, the offerer MUST insert an SDP sctpmap attribute associated
with the "m=" line.

If an offerer, in a subsequent offer, wants to disable the CLUE Data
Channel, it assigns a zero port value to the "m=" line describing the
SCTPoDTLS association used to realize the CLUE Data Channel.

5.5. Generating the Answer

The procedures for the answerer follow the normal procedures defined
in [RFC3264].

If the answerer receives an offer, which contains an "m=" line
describing a SCTPoDTLS association, and the answerer accepts the "m="
line, it inserts an "m=" line in the corresponding answer, and
assigns the "m=" line field values according to the procedures in
Section 4.2.

If the answerer receives an offer, which contains an "m=" line describing a SCTPoDTLS association, and the answerer does not accept the "m=" line, it inserts an "m=" line in the corresponding answer, and assigns a zero port value to the "m=" line, according to the procedures in [RFC3264].

If the answerer receives an offer, in which a zero port value has been assigned to an "m=" line describing the SCTPoDTLS association, it inserts an "m=" line in the corresponding answer, and assigns a zero port value to the "m=" line, according to the procedures in [RFC3264]

OPEN ISSUE (Q3): We need to determine whether an "m=" line describing an SCTPoDTLS association can be used together with bundle-only, in which case there will be cases where an offer with a zero port value will create a corresponding answer with a non-zero port value.

5.6. Offerer Processing of the Answer

When the offerer receives an SDP answer and, if the offerer ends up being active it MUST initiate a DTLS handshake by sending a DTLS ClientHello message on the negotiated media stream, towards the IP address and port of the answerer.

5.7. Modifying the Session

Once an offer/answer exchange has been completed, either endpoint MAY send a new offer in order to modify the session. The endpoints can reuse the existing SCTPoDTLS association if the key fingerprint values and transport parameters indicated by each endpoint are unchanged are unchanged. Otherwise, following the rules as for the initial offer/answer exchange, the endpoints can negotiate and create a new SCTPoDTLS association and, once created, delete the previous SCTPoDTLS association, following the same rules of for the initial offer/answer exchange.

If an offerer wants to disable the CLUE Data Channel in an offer, it assigns a zero port value to the "m=" line representing the SCTPoDTLS association used to realize the CLUE Data channel.

5.8. Example

```
a=group:CLUE 3
m=application 54111 SCTP/DTLS 54111
a=sctpmap:54111 webrtc-datachannel
a=mid:3
```

Figure 1: SDP Media Description for a CLUE Data Channel

6. Security Considerations

This specification does not introduce new security considerations, in
addition to those defined in [ref-to-data-channel] and [ref-to-data-
protocol]. Security considerations associated with the CLUE protocol
are defined in [ref-to-clue-protocol].

7. IANA Considerations

[RFC EDITOR NOTE: Please replace RFC-XXXX with the RFC number of this
document.]

8. Acknowledgments

Thanks to Paul Kyzivat and Christian Groves for comments on the
document.

9. Change Log

[RFC EDITOR NOTE: Please remove this section when publishing]

Changes from draft-ietf-clue-datachannel-01

o   Support of interleaving "MUST"->"SHOULD".
o   Example updated.
o   Reference update.

Changes from draft-ietf-clue-datachannel-00

o   SDP Offer/Answer procedures structures according to RFC 3264.
o   Reference update.

Changes from draft-holmberg-clue-datachannel-04

o   Draft submitted as draft-ietf-clue-data-channel-00.
o   Editorial nits fixed.
o   Changes based on comments from Paul Kyzivat (http://www.ietf.org/
    mail-archive/web/clue/current/msg03559.html).
o   - Proto value fixed.
o   - Explicit text that the partial reliability and limited
    retransmission policies MUST NOT be used.
o   - Added open issue on whether the DCEP 'protocol' field value for
    CLUE should contain a version number.
o   - Removed paragraph saying that an offerer must not insert more
    than one m- line describing an SCTPoDTLS association to be used to
    realize a CLUE Data Channel, as the draft already states that only
    one CLUE Data Channel per CLUE session shall be opened.

o - Added reference to draft-ietf-rtcweb-data-protocol regarding
   details on reseting SCTP streams.
o - Added text saying that the value of the DCEP 'channel type' MUST
   be DATA_CHANNEL_RELIABLE.
o - Clarified that DCEP must be supported, and used in the absence
   of another mechanism for opening a CLUE Data Channel.

   Changes from draft-holmberg-clue-datachannel-03

o Procedures updated, based on WG agreement (IETF#89) to use DCEP
   for the CLUE data channel.
o Procedures updated, based on WG agreement (IETF#89) that offerer
   is responsible for sending DCEP DATA_CHANNEL_OPEN.
o Editorial changes, and alignments caused by changes in referenced
   specifications.

   Changes from draft-holmberg-clue-datachannel-02

o PPID value for CLUE messages added
o References updated

   Changes from draft-holmberg-clue-datachannel-01

o More text added

   Changes from draft-holmberg-clue-datachannel-00

o Editorial corrections based on comments from Paul K

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119, March 1997.

[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.

[RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC
           4960, September 2007.

   [RFC5061] Stewart, R., Xie, Q., Tuexen, M., Maruyama, S., and M.
             Kozuka, "Stream Control Transmission Protocol (SCTP)
             Dynamic Address Reconfiguration", RFC 5061, September
             2007.

   [RFC6525] Stewart, R., Tuexen, M., and P. Lei, "Stream Control
             Transmission Protocol (SCTP) Stream Reconfiguration", RFC
             6525, February 2012.

   [I-D.ietf-clue-protocol]
             Presta, R. and S. Romano, "CLUE protocol", draft-ietf-
             clue-protocol-02.txt (work in progress), October 2014.

   [I-D.ietf-tsvwg-sctp-dtls-encaps]
             Tuexen, M., Stewart, R., Jesup, R., and S. Loreto, "DTLS
             Encapsulation of SCTP Packets", draft-ietf-tsvwg-sctp-
             dtls-encaps-05.txt (work in progress), July 2014.

   [I-D.ietf-rtcweb-data-channel]
             Jesup, R., Loreto, S., and M. Tuexen, "WebRTC Data
             Channels", draft-ietf-rtcweb-data-channel-12.txt (work in
             progress), September 2014.

   [I-D.ietf-rtcweb-data-protocol]
             Jesup, R., Loreto, S., and M. Tuexen, "WebRTC Data Channel
             Establishment Protocol", draft-ietf-rtcweb-data-protocol-
             08.txt (work in progress), September 2014.

   [I-D.ietf-tsvwg-sctp-ndata]
             Stewart, R., Tuexen, M., Loreto, S., and R. Seggelmann,
             "Stream Schedulers and a New Data Chunk for the Stream
             Control Transmission Protocol", draft-ietf-tsvwg-sctp-
             ndata-01.txt (work in progress), July 2014.

   [I-D.ietf-tsvwg-sctp-prpolicies]
             Tuexen, M., Seggelmann, R., Stewart, R., and S. Loreto,
             "Additional Policies for the Partial Reliability Extension
             of the Stream Control Transmission Protocol", draft-ietf-
             tsvwg-sctp-prpolicies-04.txt (work in progress), September
             2014.

10.2. Informative References

   [RFC3758] Stewart, R., Ramalho, M., Xie, Q., Tuexen, M., and P.
             Conrad, "Stream Control Transmission Protocol (SCTP)
             Partial Reliability Extension", RFC 3758, May 2004.

    [I-D.ejzak-mmusic-data-channel-sdpneg]
               Drage, K., Makaraju, R., Ejzak, R., and J. Marcon, "SDP-
               based WebRTC data channel negotiation", draft-ejzak-
               mmusic-data-channel-sdpneg-01.txt (work in progress),
               October 2014.

Author's Address

    Christer Holmberg
    Ericsson
    Hirsalantie 11
    Jorvas 02420
    Finland

    Email: christer.holmberg@ericsson.com