Stream Control Transmission Protocol (SCTP)-Based Media Transport in the
                  Session Description Protocol (SDP)
                    draft-ietf-mmusic-sctp-sdp-14

Abstract

   SCTP (Stream Control Transmission Protocol) is a transport protocol
   used to establish associations between two endpoints.

   This specification describes how to describe SCTP associations using
   the Session Description Protocol (SDP), and defines the following new
   SDP Media Description protocol identifiers (proto values):'SCTP',
   'SCTP/DTLS', 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP'.

   The specification also describes how to use the new proto values
   together with the SDP Offer/Answer mechanism in order to negotiate
   and establish SCTP associations, and how to indicate the SCTP
   application usage.

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 September 6, 2015.

Copyright Notice

Table of Contents

1. Introduction

   SDP (Session Description Protocol) [RFC4566] provides a general-
   purpose format for describing multimedia sessions in announcements or
   invitations. TCP-Based Media Transport in the Session Description
   Protocol (SDP) [RFC4145] specifies a general mechanism for describing
   and establishing TCP [RFC0793] streams. Connection-Oriented Media
   Transport over the Transport Layer Security (TLS) Protocol in SDP
   [RFC4572] extends RFC4145 [RFC4145] for describing TCP-based media
   streams that are protected using TLS.

   SCTP (Stream Control Transmission Protocol) [RFC4960] is a transport
   protocol used to establish associations between two endpoints.

   This specification defines how to describe SCTP associations using
   the Session Description Protocol (SDP) [RFC4566], and defines the
   following new SDP Media Description [RFC4566] protocol identifiers
   (proto values):'SCTP', 'SCTP/DTLS', 'UDP/DTLS/SCTP' and 'TCP/DTLS/
   SCTP'.

   The specification also describes how to use the new proto values
   together with the SDP Offer/Answer mechanism [RFC3264] in order to
   negotiate and establish SCTP associations, and how to indicate the
   SCTP application usage.

   NOTE: TLS is designed to run on top of a byte-stream oriented
   transport protocol providing a reliable, in-sequence delivery like
   TCP. [RFC6083] presents serious limitations with transporting SCTP
   on top of TLS. Therefore, defining a mechanism to negotiate media

streams transported using SCTP on top of TLS is outside the scope of this specification.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119] and indicate requirement levels for compliant implementations.

3. SCTP Terminology

SCTP Association: A protocol relationship between SCTP endpoints, composed of the two SCTP endpoints and protocol state information including Verification Tags and the currently active set of Transmission Sequence Numbers (TSNs), etc. An association can be uniquely identified by the transport addresses used by the endpoints in the association.

SCTP Stream: 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.

SCTP Transport address: A transport address is traditionally defined by a network-layer address, a transport-layer protocol, and a transport-layer port number. In the case of SCTP running over IP, a transport address is defined by the combination of an IP address and an SCTP port number (where SCTP is the transport protocol).

4. SDP Media Descriptions

4.1. General

This section defines the following new SDP Media Description (m-line) protocol identifiers (proto values) for describing an SCTP association: 'SCTP', 'SCTP/DTLS', 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP'. The section also describes how an m- line, associated with the proto values, is created.

The following is the format for an 'm' line, as specified in RFC4566 [RFC4566]:

    m=<media> <port> <proto> <fmt> ...

The 'SCTP', 'SCTP/DTLS', 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP' proto values are similar to both the 'UDP' and 'TCP' proto values in that

they only describe the transport-layer protocol and not the upper-
layer protocol.

NOTE: When the 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP' proto values are
used, the underlying transport protocol is respectively UDP and TCP;
SCTP is carried on top of DTLS which is on top of those transport-
layer protocols.

The m- line fmt value, identifying the application-layer protocol,
MUST be registered by IANA.

4.2. Protocol Identifiers

The new proto values are defined as below:

o The 'SCTP' proto value describes an SCTP association, as defined
   in [RFC4960].

o The 'SCTP/DTLS' proto value describes a Datagram Transport Layer
   Security (DTLS) [RFC6347] connection on top of an SCTP
   association, as defined in [RFC6083].

o The 'UDP/DTLS/SCTP' proto value describes an SCTP association on
   top of a DTLS connection on top of UDP, as defined in Section 7.

o The 'TCP/DTLS/SCTP' proto value describes an SCTP association on
   top of a DTLS connection on top of TCP, as defined in Section 8.

4.3. Media Format Management

[RFC4566] defines that specifications defining new proto values must
define the rules by which their media format (fmt) namespace is
managed. Use of an existing MIME subtype for the format is
encouraged. If no MIME subtype exists, it is recommended that a
suitable one is registered through the IETF process [RFC6838]
[RFC4289] by production of, or reference to, a standards-track RFC
that defines the transport protocol for the format.

An m- line with a proto value of 'SCTP', 'SCTP/DTLS', 'UDP/DTLS/SCTP'
or 'TCP/DTLS/SCTP' always describe a single SCTP association.

In addition, such m- line MUST further indicate the application-layer
protocol using an 'fmt' identifier. There MUST be exactly one 'fmt'
value per m- line associated with the proto values defined in this
specification. The "fmt" namespace associated with those proto
values describes the generic application usage of the entire SCTP
association, including the associated SCTP streams.

   NOTE: A mechanism on how to describe, and manage, individual SCTP
   streams within an SCTP association, is outside the scope of this
   specification.

4.4. Syntax

4.4.1. General

   This section defines the ABNF [RFC5234] for the SDP media description
   when associated with any of the proto values defined in this
   document.

   This specification creates an IANA registry for 'association-usage'
   values.

4.4.2. ABNF

```
     sctp-m-line = %x6d "="
      ("application" SP sctp-port SP "SCTP"       SP fmt CRLF) /
      ("application" SP sctp-port SP "SCTP/DTLS" SP fmt CRLF) /
      ("application" SP udp-port  SP "UDP/DTLS/SCTP" SP fmt CRLF) /
          ("application" SP tcp-port  SP "TCP/DTLS/SCTP" SP fmt CRLF)

     sctp-port = port

     udp-port = port

        tcp-port = port

      fmt = association-usage

      association-usage = token
```

4.5. Example

     m=application 12345 UDP/DTLS/SCTP webrtc-datachannel
     a=max-message-size: 100000

5. SDP 'sctp-port' Attribute

5.1. General

   This section defines a new SDP media-level attribute, 'sctp-port'.
   The attribute can be associated with an SDP media description (m-
   line) with a 'UDP/DTLS/SCTP' or a 'TCP/DTLS/SCTP' proto value, in
   which case the m- line port value indicates the port of the

   underlying transport-layer protocol (UDP or TCP), on which SCTP is
   carried, and the 'sctp-port' value indicates the SCTP port.

   No default value is defined for the SDP sctp-port attribute.
   Therefore, if the attribute is not present, the associated m- line
   MUST be considered invalid.

   Usage of the SDP sctp-port attribute with other proto values is not
   specified, and MUST be discarded if received.

5.2. Syntax

   The ABNF for the SDP 'sctp-port' attribute is:

      sctp-port-attr = "a=sctp-port:" port
         port   = (1*5)DIGIT

         The SCTP port range is between 0 and 65535 (both included).
         Leading zeroes MUST NOT be used.

5.3. Mux Category

   The mux category [I-D.ietf-mmusic-sdp-mux-attributes] for the SDP
   sctp-port' attribute is SPECIAL. Usage of the attribute is only
   applicable when associated with 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP'
   proto value m- lines.

   As the usage of multiple SCTP associations on top of a single DTLS
   connection is outside the scope of this specification, no mux rules
   are specified for the 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP' proto
   values. Future extensions, that define how to negotiate multiplexing
   of multiple SCTP associations of top of a single DTLS connection,
   need to also define the mux rules for the attribute.

6. SDP 'max-message-size' Attribute

6.1. General

   This section defines a new SDP media-level attribute, 'max-message-
   size'. The attribute can be associated with an m- line to indicate
   the maximum message size (indicated in bytes) that an SCTP endpoint
   is willing to receive on the SCTP association associated with the m-
   line. Different attribute values can be used in each direction.

   The remote peer MUST assume that larger messages will be rejected by
   the SCTP endpoint. SCTP endpoints need to decide on appropriate

behavior in case a message that exceeds the maximum size needs to be
sent.

If the SDP 'max-message-size' attribute contains a maximum message
size value of zero, it indicates the SCTP endpoint will handle
messages of any size, subject to memory capacity etc.

If the SDP 'max-message-size' attribute is not present, the default
value is 64K.

NOTE: This specification only defines the usage of the SDP 'max-
message-size' attribute when associated with an m- line containing
one of the following proto values: 'SCTP', 'SCTP/DTLS', 'UDP/DTLS/
SCTP' or 'TCP/DTLS/SCTP'. Usage of the attribute with other proto
values needs to be defined in a separate specification.

6.2. Syntax

The ABNF for the SDP 'max-message-size' attribute is:

```
max-message-size-attr =  "a=max-message-size:" max-message-size
max-message-size      =  1*DIGIT

    Leading zeroes MUST NOT be used.
```

6.3. Mux Category

The mux category for the SDP 'max-message-size' attribute is SPECIAL.
The mux rules depends on the proto value of the associated m- line.
If the proto value is 'SCTP' or 'SCTP/DTLS' the rules are identical
to the rules associated with the TRANSPORT mux category.

As the usage of multiple SCTP associations on top of a single DTLS
connection is outside the scope of this specification, no mux rules
are specified for the 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP' proto
values.

7. UDP/DTLS/SCTP Transport Realization

The UDP/DTLS/SCTP transport is realized as described below:

o SCTP on top of DTLS is realized according to the procedures
   defined in [I-D.ietf-tsvwg-sctp-dtls-encaps]; and

o DTLS on top of UDP is realized according to the procedures in
   defined in [RFC6347].

NOTE: While [I-D.ietf-tsvwg-sctp-dtls-encaps] allows multiple SCTP associations on top of a single DTLS connection, the procedures in this specification only supports the negotiation of a single SCTP association on top of any given DTLS connection.

8. TCP/DTLS/SCTP Transport Realization

The TCP/DTLS/SCTP transport is realized as described below:

o SCTP on top of DTLS is realized according to the procedures defined in [I-D.ietf-tsvwg-sctp-dtls-encaps]; and

o DTLS on top of TCP is realized using the framing method defined in [RFC4571], with DTLS packets being sent instead of RTP/RTCP packets, and SDP signaling according to the procedures defined in this specification.

NOTE: DTLS on top of TCP, without using the framing method defined in [RFC4571] is outside the scope of this specification. A separate proto value would need to be registered for such transport realization.

9. SCTP Association Management

9.1. General

The management of an SCTP association is identical to the management of a TCP connection. An SCTP endpoint MUST follow the rules in Section 6 of [RFC4145] to manage SCTP associations. Whether to use the SCTP ordered or unordered delivery service is up to the applications using the SCTP association, and this specification does not define a mechanism to indicate the type of delivery service using SDP.

9.2. SDP sendrecv/sendonly/recvonly/inactive Attribute

This specification does not define semantics for the SDP direction attributes [RFC4566]. Unless semantics of these attributes for an SCTP association usage have been defined, SDP direction attributes MUST be discarded if present.

9.3. SDP setup Attribute

9.3.1. General

The SDP setup attribute is used to determine the 'active/passive' status of the endpoints, following the procedures for TCP in [RFC4145].

9.3.2. SCTP Association Initiation

   Both the 'active' and 'passive' endpoint MUST initiate the SCTP
   association, and MUST use the same SCTP port as client port and
   server port (in order to prevent two separate SCTP associations from
   being established).

   NOTE: The procedure above is different from TCP, where only the
   'active' endpoint initiates the TCP connection [RFC4145].

   NOTE: If the underlying transport protocol is UDP or TCP (e.g. if the
   m- line proto value is 'UDP/DTLS/SCTP' or 'TCP/DTLS/SCTP'), when the
   SCTP association is established it is assumed that any NAT traversal
   procedures for the underlying transport protocol has successfully
   been performed.

   If the m- line proto value is 'TCP/DTLS/SCTP', the 'active' endpoint
   only MUST initiate the TCP connection, following the procedures in
   [RFC4145]. Both endpoints MUST still initiate the SCTP association
   on top of the TCP connection.

9.3.3. TLS Role Determination

   If the m- line proto value is 'SCTP/DTLS', 'UDP/DTLS/SCTP' or
   'TCP/DTLS/SCTP', the 'active/passive' status is used to determine the
   (D)TLS roles of the endpoints. Following the procedures in
   [RFC4572], the 'active' endpoint will take the (D)TLS client role.

   Once the DTLS connection has been established, the endpoints MUST NOT
   modify (as result of an offer/answer exchange) the TLS roles, or the
   'active/passive' status, of the endpoints, unless the underlying
   transport protocol is also modified (e.g. if an IP address- or port
   value associated with the transport protocol is modified).

   If the underlying transport protocol is modified, the endpoints MUST
   establish a new DTLS connection. In such case the 'active/passive'
   status of the endpoints will again be determined following the
   procedures in [RFC4145], and the new status will be used to determine
   the (D)TLS roles of the endpoints associated with the new DTLS
   connection.

   NOTE: The procedure above is identical to the one defined for SRTP-
   DTLS in [RFC5763].

9.4. SDP connection Attribute

   The SDP connection attribute is used following the procedures in
   [RFC4145], with the additional SCTP specific considerations described
   in this section.

   If the m- line proto value is 'TCP/DTLS/SCTP', an SDP connection
   attribute associated with that m- line applies to both the SCTP
   association and the TCP connection. Therefore, an attribute 'new'
   value indicates that both a new SCTP association and new TCP
   connection have to be established, following the procedures in
   [RFC4145].

   NOTE: This specification does not define a mechanism which allows re-
   establishing of a new SCTP association, while maintaining the
   underlying TCP connection.

   The SDP connection attribute value does not automatically impact an
   existing DTLS connection. Section 9.3.3 describes in which cases a
   new DTLS connections will have to be re-established.

10. SDP Offer/Answer Procedures

10.1. General

   This section defines the SDP Offer/Answer [RFC3264] procedures for
   negotiating and establishing an SCTP association. Unless explicitly
   stated, the procedures apply to all m- line proto values ('SCTP',
   'SCTP/DTLS', 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP') defined in this
   specification.

   If the m- line proto value is 'SCTP/DTLS', 'UDP/DTLS/SCTP' or
   'TCP/DTLS/SCTP', each endpoint MUST provide a certificate
   fingerprint, using the SDP 'fingerprint' attribute [RFC4572], if the
   endpoint supports, and is willing to use, a cipher suite with an
   associated certificate.

   The authentication certificates are interpreted and validated as
   defined in [RFC4572]. Self-signed certificates can be used securely,
   provided that the integrity of the SDP description is assured as
   defined in [RFC4572].

   NOTE: The procedures apply to a specific m- line describing an SCTP
   association. If an offer or answer contains multiple m- lines
   describing SCTP associations, the procedures are applied separately
   to each m- line.

10.2. Generating the Initial SDP Offer

   When the offerer creates an initial offer, the offerer:

   o MUST, if the m- line proto value is 'SCTP/DTLS', 'UDP/DTLS/SCTP'
      or 'TCP/DTLS/SCTP', associate an SDP setup attribute, with an
      'actpass' value, with the m- line (see Section 9.3);

   o MUST, if the m- line proto is 'UDP/DTLS/SCTP' or 'TCP/DTLS/SCTP',
      associate an SDP 'sctp-port' attribute with the m- line (see
      Section 5);

   o MUST associate an SDP 'connection' attribute, with a 'new' value,
      with the m- line (see Section 9.4); and

   o MAY associate an SDP 'max-message-size' attribute with the m- line
      (see Section 6).

10.3. Generating the SDP Answer

   When the answerer receives an offer, which contains an m- line
   describing an SCTP association, if the answerer accepts the m- line
   it:

   o MUST insert a corresponding m- line in the answer, with an
      identical m- line proto value [RFC3264];

   o MUST, if the m- line proto value is 'SCTP/DTLS', 'UDP/DTLS/SCTP'
      or 'TCP/DTLS/SCTP', associate an SDP 'setup' attribute, with an
      'active' or 'passive' value, with the m- line (see Section 9.3);

   o MUST, if the m- line proto is 'UDP/DTLS/SCTP' or 'TCP/DTLS/SCTP',
      associate an SDP 'sctp-port' attribute with the m- line (see
      Section 5); and

   o MAY associate an SDP 'max-message-size' attribute with the m- line
      (see Section 6). The attribute value in the answer is independent
      from the value (if present) in the corresponding m- line of the
      offer.

   Once the answerer has sent the answer, the answerer:

   o MUST, if an SCTP association associated with the m- line has yet
      not been established, or if an existing SCTP association is to be
      re-established, initiate the establishing of the SCTP association;
      and

   o MUST, if the answerer is the 'active' endpoint, and if an DTLS
      connection associated with the m- line is to be established (or
      re-established), initiate the establishing of the DTLS connection
      (by sending a ClientHello message).

   If the answerer does not accept the m- line in the offer, it MUST
   assign a zero port value to the corresponding m- line in the answer.
   In addition, the answerer MUST NOT establish an SCTP association, or
   a DTLS connection, associated with the m- line.

10.4. Offerer Processing of the SDP Answer

   When the offerer receives an answer, which contains an m- line with a
   non-zero port value, describing an SCTP association, the offerer:

   o MUST, if the offerer is the 'active' endpoint, if the m- line
      proto value is 'TCP/DTLS/SCTP', and if a TCP connection used to
      carry the SCTP association has not yet been established (or if an
      existing TCP connection is to be re-established), initiate the
      establishing of the TCP connection;

   o MUST, if an SCTP association associated with the m- line has not
      yet been established (or if an existing SCTP association is to be
      re-established), initiate the establishing of the SCTP
      association; and

   o MUST, if the offerer is the 'active' endpoint, and if a DTLS
      connection associated with the m- line is to be established (or if
      an existing DTLS connection is to be re-established), initiate the
      establishing of the DTLS connection (by sending a ClientHello
      message).

   o NOTE: If the m- line proto value is 'UDP/DTLS/SCTP' or 'TCP/DTLS/
      SCTP', the underlying DTLS connection needs to be established
      before the SCTP association can be established.

   If the m- line in the answer contains a zero port value, the offerer
   MUST NOT establish a TCP connection, an SCTP association, or a DTLS
   connection, associated with the m- line.

10.5. Modifying the Session

   When an offerer sends an updated offer, in order to modify a
   previously established SCTP association, it follows the procedures in
   Section 10.2, with the following exceptions:

   o Unless the offerer wants to re-establish an existing SCTP
      association, the offerer MUST associate an SDP connection
      attribute, with an 'existing' value, with the m- line; and

   o If the offerer wants to disable a previously established SCTP
      association, it MUST assign a zero port value to the m- line
      associated with the SCTP association, following the procedures in
      [RFC3264].

11. Multihoming Considerations

   SCTP supports multihoming. An SCTP endpoint is considered multihomed
   if it has more than one IP address on which SCTP can be used. An
   SCTP endpoint inform the remote peer about its IP addresses using the
   address parameters in the INIT/INIT-ACK chunk. Therefore, when SDP
   is used to describe an SCTP association, while the "c=" line contains
   the address which was used to negotiate the SCTP association,
   multihomed SCTP endpoints might end up using other IP addresses.

   If an endpoint removes the IP address [RFC5061] that it offered in
   the SDP "c=" line associated with the SCTP association, it MUST send
   a new Offer, in which the "c=" line contains an IP address which is
   valid within the SCTP association.

   NOTE: In some network environments, intermediaries performing gate-
   and firewall control using the address information in the SDP "c="
   and "m=" lines to authorize media, and will not pass media sent using
   other addresses. In such network environments, if an SCTP endpoints
   wants to change the address information on which media is sent and
   received, it needs to send an updated Offer, in which the SDP "c="
   and "m=" lines contain the new address information.

   Multihoming is not supported when sending SCTP on top of DTLS, as
   DTLS does not expose address management of the underlying transport
   protocols (UDP or TCP) to its upper layer.

12. NAT Considerations

12.1. General

   SCTP features not present in UDP or TCP, including the checksum
   (CRC32c) value calculated on the whole packet (rather than just the
   header), and multihoming, introduce new challenges for NAT traversal.
   [I-D.ietf-behave-sctpnat] defines an SCTP specific variant of NAT,
   which provides similar features of Network Address and Port
   Translation (NAPT).

Current NATs typically do not support SCTP. [RFC6951] defines a
mechanism for sending SCTP on top of UDP, which makes it possible to
use SCTP with NATs and firewalls that do not support SCTP.

12.2. ICE Considerations

At the time of writing this specification, no procedures have been
defined for using ICE (Interactive Connectivity Establishment)
[RFC5245] together with SCTP as transport layer protocol. Such
procedures, including the associated SDP Offer/Answer procedures, are
outside the scope of this specification, and might be defined in a
future specification.

When the transport layer protocol is UDP (in case of an SCTP
association on top of a DTLS connection on top of UDP), if ICE is
used, the ICE procedures defined in [RFC5245] are used.

When the transport layer protocol is TCP (in case of an SCTP
association on top of a DTLS connection on top of TCP), if ICE is
used, the ICE procedures defined in [RFC6544] are used.

13. Examples

13.1. Establishment of UDP/DTLS/SCTP association

SDP Offer:

```
m=application 54111 UDP/DTLS/SCTP webrtc-datachannel
c=IN IP4 192.0.2.1
```
a=setup:actpass
a=connection:new
```
a=sctp-port:5000
a=max-message-size:100000
```

- The offerer indicates that the usage of the
     UDP/DTLS/SCTP association will be as defined
     for the 'webrtc-datachannel' format value.
  - The offerer UDP port value is 54111.
  - The offerer SCTP port value is 5000.
  - The offerer indicates that it can take either the
     active or the passive role.

SDP Answer:

```
m=application 64300 UDP/DTLS/SCTP webrtc-datachannel
c=IN IP4 192.0.2.2
```
a=setup:passive
```
a=sctp-port:6000
a=max-message-size:100000
```

- The answerer UDP port value is 64300.
  - The answerer SCTP port value is 6000.
  - The answerer takes the passive role.

14. Security Considerations

   [RFC4566] defines general SDP security considerations, while
   [RFC3264], [RFC4145] and [RFC4572] define security considerations
   when using the SDP offer/answer mechanism to negotiate media streams.

   [RFC4960] defines general SCTP security considerations, while
   [RFC6083] defines security considerations when using DTLS on top of
   SCTP.

   This specification does not introduce new security considerations in
   addition to those defined in the specifications listed above.

15. IANA Considerations

15.1. New SDP proto values

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

   This document updates the "Session Description Protocol (SDP)
   Parameters" registry, following the procedures in [RFC4566], by
   adding the following values to the table in the SDP "proto" field
   registry:

```
         +-------+--------------+-----------+
         | Type  |   SDP Name   | Reference |
         +-------+--------------+-----------+
         | proto |     SCTP     | [RFCXXXX] |
         | proto |   SCTP/DTLS  | [RFCXXXX] |
         | proto | UDP/DTLS/SCTP | [RFCXXXX] |
         | proto | TCP/DTLS/SCTP | [RFCXXXX] |
         +-------+--------------+-----------+
```

                Table 1: SDP "proto" field values

15.2. New SDP Attributes

15.2.1. sctp-port

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

   This document defines a new SDP media-level attribute,'sctp-port', as
   follows:

```
         Attribute name:      sctp-port
         Type of attribute:   media
         Mux category:        SPECIAL
         Subject to charset:  No
         Purpose:             Indicate the SCTP port value associated
                              with the SDP Media Description.
         Appropriate values:  Integer
         Contact name:        Christer Holmberg
         Contact e-mail:      christer.holmberg@ericsson.com
         Reference:           RFCXXXX
```

15.2.2. max-message-size

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

   This document defines a new SDP media-level attribute,'max-message-
   size', as follows:

           Attribute name: max-message-size
           Type of attribute: media
           Mux category: SPECIAL
           Subject to charset: No
           Purpose: Indicate the maximum message size that
                               an SCTP endpoint is willing to receive
                               on the SCTP association associated
                               with the SDP Media Description.
           Appropriate values: Integer
           Contact name: Christer Holmberg
           Contact e-mail: christer.holmberg@ericsson.com
           Reference: RFCXXXX

15.3. association-usage Name Registry

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

   This specification creates a new IANA registry, following the
   procedures in [RFC5226], for the "fmt" namespace associated with the
   'SCTP', 'SCTP/DTLS', 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP' protocol
   identifiers. Each "fmt" value describes the usage of an entire SCTP
   association, including all SCTP streams associated with the SCTP
   association.

   NOTE: Usage indication of individual SCTP streams is outside the
   scope of this specification.

   The "fmt" value, "association-usage", used with these "proto" is
   required. It is defined in [Section 4].

   As part of this registry, IANA maintains the following information:

   association-usage name: The identifier of the subprotocol, as will
      be used as the "fmt" value.

   association-usage reference: A reference to the document in which
      the association-usage is defined.

association-usage names are to be subject to the "First Come First
Served" IANA registration policy [RFC5226].

IANA is asked to add initial values to the registry.

```
|---------------------------------------------------------|
|        name          |              Reference            |
|---------------------------------------------------------|
| webrtc-datachannel | draft-ietf-rtcweb-data-protocol-xx  |
|---------------------------------------------------------|
```

[RFC EDITOR NOTE: Please hold the publication of this draft
until draft-ietf-rtcweb-data-protocol has been published as an RFC.
Then, replace the reference to draft-ietf-rtcweb-data-protocol
with the RFC number.]

Figure 1

16. Acknowledgments

The authors wish to thank Harald Alvestrand, Randell Jesup, Paul
Kyzivat, Michael Tuexen, Juergen Stoetzer-Bradler, Flemming Andreasen
and Ari Keranen for their comments and useful feedback.

17. Change Log

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

Changes from draft-ietf-mmusic-sctp-sdp-13

o Changes based on comments from Paul Kyzivat.

o - Text preventing usage of well-known ports removed.

o - Editorial clarification.

Changes from draft-ietf-mmusic-sctp-sdp-12

o Mux category rules added for new SDP attributes.

o Reference to draft-ietf-mmusic-sdp-mux-attributes added.

o Changes based on comments from Roman Shpount:

o - Specify that fingerprint or setup roles must not be modified,
   unless underlying transport protocol is also modified.

o Changes based on comments from Ari Keranen:

o - Editorial corrections.

o Changes based on comments from Flemming Andreasen:

o - Clarify that, if UDP/DTLS/SCTP or TCP/DTLS/SCTP is used, the
   DTLS connection is established before the SCTP association.

o - Clarify that max-message-size value is given in bytes, and that
   different values can be used per direction.

o - Section on fmtp attribute removed.

o - Editorial corrections.

Changes from draft-ietf-mmusic-sctp-sdp-11

o Example added.

Changes from draft-ietf-mmusic-sctp-sdp-10

o SDP max-message-size attribute added to IANA considerations.

o Changes based on comments from Paul Kyzivat:

o - Text about max message size removed from fmtp attribute section.

Changes from draft-ietf-mmusic-sctp-sdp-09

o 'DTLS/SCTP' split into 'UDP/DTLS/SCTP' and 'TCP/DTLS/SCTP'

o Procedures for realizing UDP/DTLS/SCTP- and TCP/DTLS/SCTP
   transports added.

Changes from draft-ietf-mmusic-sctp-sdp-08

o Default SCTP port removed:

o - Usage of SDP sctp-port attribute mandatory.

o SDP max-message-size attribute defined:

o - Attribute definition.

o - SDP Offer/Answer procedures.

o Text about SDP direction attributes added.

   o Text about TLS role determination added.

18. References

18.1. Normative References

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

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

   [RFC4145] Yon, D. and G. Camarillo, "TCP-Based Media Transport in
              the Session Description Protocol (SDP)", RFC 4145,
              September 2005.

   [RFC4289] Freed, N. and J. Klensin, "Multipurpose Internet Mail
              Extensions (MIME) Part Four: Registration Procedures", BCP
              13, RFC 4289, December 2005.

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

   [RFC4571] Lazzaro, J., "Framing Real-time Transport Protocol (RTP)
              and RTP Control Protocol (RTCP) Packets over Connection-
              Oriented Transport", RFC 4571, July 2006.

   [RFC4572] Lennox, J., "Connection-Oriented Media Transport over the
              Transport Layer Security (TLS) Protocol in the Session
              Description Protocol (SDP)", RFC 4572, July 2006.

   [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.

   [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an
              IANA Considerations Section in RFCs", BCP 26, RFC 5226,
              May 2008.

   [RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax
              Specifications: ABNF", STD 68, RFC 5234, January 2008.

   [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security
              (TLS) Protocol Version 1.2", RFC 5246, August 2008.

   [RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer
              Security Version 1.2", RFC 6347, January 2012.

   [RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type
              Specifications and Registration Procedures", BCP 13, RFC
              6838, January 2013.

   [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-09 (work in progress), January 2015.

   [I-D.ietf-mmusic-sdp-mux-attributes]
              Nandakumar, S., "A Framework for SDP Attributes when
              Multiplexing", draft-ietf-mmusic-sdp-mux-attributes-08
              (work in progress), January 2015.

18.2. Informative References

   [RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC
              793, September 1981.

   [RFC5245] Rosenberg, J., "Interactive Connectivity Establishment
              (ICE): A Protocol for Network Address Translator (NAT)
              Traversal for Offer/Answer Protocols", RFC 5245, April
              2010.

   [RFC5763] Fischl, J., Tschofenig, H., and E. Rescorla, "Framework
              for Establishing a Secure Real-time Transport Protocol
              (SRTP) Security Context Using Datagram Transport Layer
              Security (DTLS)", RFC 5763, May 2010.

   [RFC6083] Tuexen, M., Seggelmann, R., and E. Rescorla, "Datagram
              Transport Layer Security (DTLS) for Stream Control
              Transmission Protocol (SCTP)", RFC 6083, January 2011.

   [RFC6544] Rosenberg, J., Keranen, A., Lowekamp, B., and A. Roach,
              "TCP Candidates with Interactive Connectivity
              Establishment (ICE)", RFC 6544, March 2012.

   [RFC6951] Tuexen, M. and R. Stewart, "UDP Encapsulation of Stream
              Control Transmission Protocol (SCTP) Packets for End-Host
              to End-Host Communication", RFC 6951, May 2013.

   [I-D.ietf-behave-sctpnat]
              Stewart, R., Tuexen, M., and I. Ruengeler, "Stream Control
              Transmission Protocol (SCTP) Network Address Translation",
              draft-ietf-behave-sctpnat-09 (work in progress), September
              2013.

Authors' Addresses

   Christer Holmberg
   Ericsson
   Hirsalantie 11
   Jorvas 02420
   Finland

   Email: christer.holmberg@ericsson.com

   Salvatore Loreto
   Ericsson
   Hirsalantie 11
   Jorvas 02420
   Finland

   Email: Salvatore.Loreto@ericsson.com

   Gonzalo Camarillo
   Ericsson
   Hirsalantie 11
   Jorvas 02420
   Finland

   Email: Gonzalo.Camarillo@ericsson.com