

MMUSIC  
Internet-Draft  
Intended status: Standards Track  
Expires: June 22, 2015

C. Holmberg  
S. Loreto  
G. Camarillo  
Ericsson  
December 19, 2014

Stream Control Transmission Protocol (SCTP)-Based Media Transport in the  
Session Description Protocol (SDP)  
[draft-ietf-mmusic-sctp-sdp-10](#)

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 June 22, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">4</a>
<a href="#">3.</a>	SCTP Terminology . . . . .	<a href="#">4</a>
<a href="#">4.</a>	SDP Media Descriptions . . . . .	<a href="#">4</a>
<a href="#">4.1.</a>	General . . . . .	<a href="#">4</a>
<a href="#">4.2.</a>	Protocol Identifiers . . . . .	<a href="#">5</a>
<a href="#">4.3.</a>	Media Format Management . . . . .	<a href="#">5</a>
<a href="#">4.4.</a>	Syntax . . . . .	<a href="#">6</a>
<a href="#">4.5.</a>	Example . . . . .	<a href="#">6</a>
<a href="#">5.</a>	SDP 'sctp-port' Attribute . . . . .	<a href="#">6</a>
<a href="#">5.1.</a>	General . . . . .	<a href="#">6</a>
<a href="#">5.2.</a>	Syntax . . . . .	<a href="#">6</a>
<a href="#">6.</a>	SDP 'max-message-size' Attribute . . . . .	<a href="#">7</a>
<a href="#">6.1.</a>	General . . . . .	<a href="#">7</a>
<a href="#">6.2.</a>	Syntax . . . . .	<a href="#">7</a>
<a href="#">7.</a>	SDP 'fmtp' Attribute . . . . .	<a href="#">7</a>
<a href="#">7.1.</a>	General . . . . .	<a href="#">7</a>
<a href="#">7.2.</a>	Syntax . . . . .	<a href="#">8</a>
<a href="#">8.</a>	UDP/DTLS/SCTP Transport Realization . . . . .	<a href="#">8</a>
<a href="#">9.</a>	TCP/DTLS/SCTP Transport Realization . . . . .	<a href="#">8</a>
<a href="#">10.</a>	SCTP Association Management . . . . .	<a href="#">8</a>
<a href="#">10.1.</a>	General . . . . .	<a href="#">8</a>
<a href="#">10.2.</a>	SDP sendrecv/sendonly/sendrecv/inactive Attribute . . . . .	<a href="#">9</a>
<a href="#">10.3.</a>	SDP setup Attribute . . . . .	<a href="#">9</a>
<a href="#">10.3.1.</a>	General . . . . .	<a href="#">9</a>
<a href="#">10.3.2.</a>	SCTP Association Initiation . . . . .	<a href="#">9</a>
<a href="#">10.3.3.</a>	TLS Role Determination . . . . .	<a href="#">9</a>
<a href="#">10.4.</a>	SDP connection Attribute . . . . .	<a href="#">10</a>
<a href="#">11.</a>	SDP Offer/Answer Procedures . . . . .	<a href="#">10</a>
<a href="#">11.1.</a>	General . . . . .	<a href="#">10</a>
<a href="#">11.2.</a>	Generating the Initial SDP Offer . . . . .	<a href="#">11</a>
<a href="#">11.3.</a>	Generating the SDP Answer . . . . .	<a href="#">11</a>
<a href="#">11.4.</a>	Offerer Processing of the SDP Answer . . . . .	<a href="#">12</a>
<a href="#">11.5.</a>	Modifying the Session . . . . .	<a href="#">13</a>
<a href="#">12.</a>	Multihoming Considerations . . . . .	<a href="#">13</a>
<a href="#">13.</a>	NAT Considerations . . . . .	<a href="#">14</a>



<a href="#">13.1.</a>	General . . . . .	<a href="#">14</a>
<a href="#">13.2.</a>	ICE Considerations . . . . .	<a href="#">14</a>
<a href="#">14.</a>	Examples . . . . .	<a href="#">14</a>
<a href="#">15.</a>	Security Considerations . . . . .	<a href="#">14</a>
<a href="#">16.</a>	IANA Considerations . . . . .	<a href="#">14</a>
<a href="#">16.1.</a>	New SDP proto values . . . . .	<a href="#">14</a>
<a href="#">16.2.</a>	New SDP Attribute . . . . .	<a href="#">15</a>
<a href="#">16.3.</a>	association-usage Name Registry . . . . .	<a href="#">15</a>
<a href="#">17.</a>	Acknowledgments . . . . .	<a href="#">16</a>
<a href="#">18.</a>	Change Log . . . . .	<a href="#">16</a>
<a href="#">19.</a>	References . . . . .	<a href="#">17</a>
<a href="#">19.1.</a>	Normative References . . . . .	<a href="#">17</a>
<a href="#">19.2.</a>	Informative References . . . . .	<a href="#">18</a>
	Authors' Addresses . . . . .	<a href="#">19</a>

## **[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 (Transmission Control Protocol) [[RFC5246](#)] streams. Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP) [[RFC4572](#)] extends [RFC4145](#) [[RFC4145](#)] for describing TCP-based media streams that are protected using TLS.

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) [[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. Two SCTP endpoints MUST NOT have more than one SCTP association between them at any given time.

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 either UDP or TCP, SCTP is carried on top of either 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 8](#).
- 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 9](#).

#### **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**

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

```
sctp-port = port
```

```
udp-port = port
```

```
sctp-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 descriptor (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 transport-layer protocol (UDP or TCP), on which SCTP is carried.

If the SDP sctp-port attribute is not present, the m- line MUST be discarded.

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

#### [5.2.](#)    **Syntax**

```
sctp-port-attr = "a=sctp-port:" port
port           = 1*DIGIT
```



## **6.   SDP 'max-message-size' Attribute**

### **6.1.   General**

The SDP 'max-message-size' attribute can be associated with an m-line to indicate the maximum message size that an SCTP endpoint is willing to receive on the SCTP association associated with the m-line.

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.

### **6.2.   Syntax**

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

## **7.   SDP 'fmtp' Attribute**

### **7.1.   General**

The SDP 'fmtp' attribute can be used with an m- line, associated with an SCTP association, to indicate the maximum message size that an SCTP endpoint is willing to receive, for a particular SCTP association usage, on that SCTP association.

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 'fmtp' 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 'fmtp' 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 field 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.

## **7.2. Syntax**

```
sctpmap-attr      = "a=fmtp:" association-usage [max-message-size]
max-message-size  = "max-message-size" EQUALS 1*DIGIT
```

## **8. 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](#)].

## **9. 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](#)].

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.

## **10. SCTP Association Management**

### **10.1. General**

The management of an SCTP association is identical to the management of a TCP connection. An SCTP endpoints 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.

### **10.2.   SDP sendrecv/sendonly/sendrecv/inactive Attribute**

This specification does not define semantics for the SDP direction attributes [[RFC4566](#)]. Specifications for an individual SCTP association usage MAY define how the attributes can be used with that usage. Unless semantics of these attributes for an SCTP association usage have been defined, SDP direction attributes MUST be discarded if present.

### **10.3.   SDP setup Attribute**

#### **10.3.1.   General**

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

#### **10.3.2.   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](#)].

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

#### **10.3.3.   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 TLS roles of the endpoints. Following the procedures in [[RFC4572](#)], the 'active' endpoint will take the TLS client role.

Once a DTLS connection has been established, if the 'active/passive' status of the endpoints change (as result of an offer/answer transaction) during a session, a new DTLS connection MUST be established. Therefore, endpoints SHOULD NOT change the 'active/passive' status during a session, unless they want to establish a new DTLS connection.





If the transport parameters or the key fingerprints change, 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 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 [\[RFC5763\]](#).

#### **[10.4.](#)    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 a 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 TCP connection.

The SDP connection attribute value does not automatically impact an existing DTLS connection. [Section 10.3.3](#) describes in which cases a new DTLS connections will be established.

NOTE: If the m- line proto value is 'SCTP/DTLS', and if the SCTP association is re-established, the DTLS connection also needs to be re-established.

### **[11.](#)    SDP Offer/Answer Procedures**

#### **[11.1.](#)    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 [\[RFC4145\]](#), 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.

### **[11.2.](#) 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 [\[Section 10.3\]](#), with an 'actpass' value, with the m- line;
- o MUST, if the m- line proto is 'UDP/DTLS/SCTP' or 'TCP/DTLS/SCTP', associate an SDP 'sctp-port' attribute [\[Section 5\]](#) with the m- line;
- o MUST associate an SDP 'connection' attribute [\[Section 10.4\]](#), with a 'new' value, with the m- line; and
- o MAY associate an SDP 'max-message-size' attribute [\[Section 7\]](#) with the m- line.

### **[11.3.](#) 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 [\[Section 10.3\]](#), with an 'active' or 'passive' value, with the m- line;
- o MUST, if the m- line proto is 'UDP/DTLS/SCTP' or 'TCP/DTLS/SCTP', associate an SDP 'sctp-port' attribute [\[Section 5\]](#) with the m- line; and



- o MAY associate an SDP 'max-message-size' attribute [[Section 7](#)] with the m- line.

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.

#### **11.4. 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 is 'TCP/DTLS/SCTP', and if a TCP connection used to carry the SCTP association has yet not 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 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 offerer is the 'active' endpoint, and if an 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).

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.



### **11.5.    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 11.2](#), 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 [\[RFC3264\]](#).

NOTE: Different SCTP association usages might define protocol procedures etc that need to be performed before an SCTP association is terminated. Such procedures are outside the scope of this specification.

## **12.    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 with is valid within the SCTP association.

NOTE: In some network environments, intermediaries performing gate- and firewall control use 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 environment, 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 to its upper layer.





## **13. NAT Considerations**

### **13.1. 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.

### **13.2. ICE Considerations**

At the time of writing this specification, no procedures have been defined for using ICE (Interactive Connectivity Establishment) [\[RFC5768\]](#) together with SCTP. Such procedures, including the associated SDP Offer/Answer procedures, are outside the scope of this specification, and might be defined in a future specification.

## **14. Examples**

TODO: ADD EXAMPLES HERE

## **15. 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. security considerations on SCTP in general, 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.

## **16. IANA Considerations**

### **16.1. 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]
TCP/DTLS/SCTP	[RFCXXXX]	

Table 1: SDP "proto" field values

### **16.2. New SDP Attribute**

[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
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

```

### **16.3. 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 in the <sctp-fmt> subfield.

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	<a href="#">draft-ietf-rtcweb-data-protocol-xx</a>

Figure 1

## 17. Acknowledgments

The authors wish to thank Harald Alvestrand, Randell Jesup, Paul Kyzivat, Michael Tuexen for their comments and useful feedback.

## 18. Change Log

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

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.

## **19. References**

### **19.1. 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.
- [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-06](#) (work in progress), November 2014.

## **19.2. Informative References**

- [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.
- [RFC5768] Rosenberg, J., "Indicating Support for Interactive Connectivity Establishment (ICE) in the Session Initiation Protocol (SIP)", [RFC 5768](#), April 2010.
- [RFC6083] Tuexen, M., Seggelmann, R., and E. Rescorla, "Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)", [RFC 6083](#), January 2011.
- [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](mailto:christer.holmberg@ericsson.com)

Salvatore Loreto  
Ericsson  
Hirsalantie 11  
Jorvas 02420  
Finland

Email: [Salvatore.Loreto@ericsson.com](mailto:Salvatore.Loreto@ericsson.com)

Gonzalo Camarillo  
Ericsson  
Hirsalantie 11  
Jorvas 02420  
Finland

Email: [Gonzalo.Camarillo@ericsson.com](mailto:Gonzalo.Camarillo@ericsson.com)

