

MMUSIC
Internet-Draft
Intended status: Standards Track
Expires: September 15, 2011

S. Loreto
G. Camarillo
Ericsson
March 14, 2011

Stream Control Transmission Protocol (SCTP)-Based Media Transport in the
Session Description Protocol (SDP)
[draft-loreto-mmusic-sctp-sdp-07](#)

Abstract

SCTP (Stream Control Transmission Protocol) is a transport protocol used to establish associations between two endpoints. This document describes how to express media transport over SCTP in SDP (Session Description Protocol). This document defines the 'SCTP' and 'SCTP/DTLS' protocol identifiers for SDP.

Status of this Memo

This Internet-Draft is submitted to IETF 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 15, 2011.

Copyright Notice

Copyright (c) 2011 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

1.	Introduction	3
2.	Terminology	3
3.	Protocol Identifier	3
4.	The Setup and Connection Attributes and Association Management	4
5.	Multihoming	4
6.	Examples	5
6.1.	Actpass/Passive	5
6.2.	Existing Connection Reuse	6
6.3.	SDP description for DTLS Connection	6
7.	Network Address Translators (NAT) Considerations	7
8.	Security Considerations	7
9.	IANA Considerations	8
10.	Normative References	8
	Authors' Addresses	9

1. Introduction

SDP (Session Description Protocol) [[RFC4566](#)] provides a general-purpose format for describing multimedia sessions in announcements or invitations. [RFC4145](#) [[RFC4145](#)] specifies a general mechanism for describing and establishing TCP (Transmission Control Protocol) streams. [RFC 4572](#) [[RFC4572](#)] extends [RFC4145](#) [[RFC4145](#)] for describing TCP-based media streams that are protected using TLS (Transport Layer Security) [[RFC5246](#)].

This document defines a new protocol identifier, 'SCTP', to describe SCTP-based [[RFC4960](#)] media streams. Additionally, this document specifies the use of the 'setup' and 'connection' SDP attributes to establish SCTP associations. These attributes were defined in [RFC4145](#) [[RFC4145](#)] for TCP. This document discusses their use with SCTP.

Additionally this document defines a new protocol identifier, 'SCTP/DTLS', to establish secure SCTP-based media streams over DTLS (Datagram Transport Layer Security) [[RFC4347](#)], as specified in [[RFC6083](#)], using SDP. The authentication certificates are interpreted and validated as defined in [RFC4572](#) [[RFC4572](#)]. Self-signed certificates can be used securely, provided that the integrity of the SDP description is assured as defined in [RFC4572](#) [[RFC4572](#)].

TLS is designed to run on top of a byte-stream oriented transport protocol providing a reliable, in-sequence delivery like TCP. Since no-one so far has implemented SCTP over TLS, due to some serious limitations described in [[RFC6083](#)], this document does not make use of TLS over SCTP as described in [RFC3436](#) [[RFC3436](#)].

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. Protocol Identifier

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

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

This document defines two new values for the 'proto' field: 'SCTP' and 'SCTP/DTLS'.

The 'SCTP' protocol identifier is similar to both the 'UDP' and 'TCP' protocol identifiers in that it only describes the transport protocol and not the upper-layer protocol. Media described using an 'm' line containing the 'SCTP' protocol identifier are carried using SCTP [[RFC4960](#)].

The 'SCTP/DTLS' protocol identifier indicates that the media described will use the Datagram Transport Layer Security (DTLS) [[RFC4347](#)] over SCTP as specified in [[RFC6083](#)].

An 'm' line that specifies 'SCTP' or 'SCTP/DTLS' MUST further qualify the application-layer protocol using an fmt identifier.

An 'm' line that specifies 'SCTP/DTLS' MUST further provide a certificate fingerprint. An SDP attribute (an 'a' line) is used to transport and exchange end point certificate. The authentication certificates are interpreted and validated as defined in [[RFC4572](#)].

4. The Setup and Connection Attributes and Association Management

The use of the 'setup' and 'connection' attributes in the context of an SCTP association is identical to the use of these attributes in the context of a TCP connection. That is, SCTP endpoints MUST follow the rules in Sections 4 and 5 of [RFC 4145](#) [[RFC4145](#)] when it comes to the use of the 'setup' and 'connection' attributes in offer/answer

[\[RFC3264\]](#) exchanges.

The management of an SCTP association is identical to the management of a TCP connection. That is, SCTP endpoints MUST follow the rules in [Section 6 of RFC 4145](#) [\[RFC4145\]](#) to manage SCTP associations. Whether to use the SCTP ordered or unordered delivery service is up to the applications using the SCTP association.

5. Multihoming

An SCTP endpoint, unlike a TCP endpoint, can be multihomed. An SCTP endpoint is considered to be multihomed if it has more than one IP address. A multihomed SCTP endpoint informs a remote SCTP endpoint about all its IP addresses using the address parameters of the INIT or the INIT-ACK chunk (depending on whether or not the multihomed endpoint is the one initiating the establishment of the association). Therefore, once the address provided in the 'c' line has been used to establish the SCTP association (i.e., to send the INIT chunk),

address management is performed using SCTP. This means that two SCTP endpoints can use addresses that were not listed in the 'c' line but that were negotiated using SCTP mechanisms.

Some intermediaries performing firewall control use the addresses in offer/answer exchanges to perform media authorization. That is, they will not let media through unless it is sent to the address in the 'c' line.

The SCTP endpoints MAY choose to use the main address all the time (e.g., they do not send retransmissions to a backup address) and to send a re-INVITE every time they change that address.

However not using non-primary paths for retransmission means not to utilize the multi-homing feature of SCTP for resilience. Therefore, the SCTP endpoints MAY use the 'candidate' SDP attribute to disclosure, to intermediaries performing firewall control, all its alternative IP addresses; this will avoid the need for the SCTP endpoints to send a re-INVITE every time they change the primary path.

6. Examples

The following examples show the use of the 'setup' and 'connection' SDP attributes. As discussed in [Section 4](#), the use of these attributes with an SCTP association is identical to their use with a TCP connection. For the purpose of brevity, the main portion of the session description is omitted in the examples, which only show 'm' lines and their attributes (including 'c' lines).

6.1. Actpass/Passive

An offerer at 192.0.2.2 signals its availability for an SCTP association at SCTP port 54111. Additionally, this offerer is also willing to initiate the SCTP association:

```
m=image 54111 SCTP *  
c=IN IP4 192.0.2.2  
a=setup:actpass  
a=connection:new
```

Figure 1

The endpoint at 192.0.2.1 responds with the following description:

```
m=image 54321 SCTP *  
c=IN IP4 192.0.2.1  
a=setup:passive  
a=connection:new
```

Figure 2

This will cause the offerer (at 192.0.2.2) to initiate an SCTP association to port 54321 at 192.0.2.1.

6.2. Existing Connection Reuse

Subsequent to the exchange in [Section 6.1](#), another offer/answer exchange is initiated in the opposite direction. The endpoint at 192.0.2.1, which now acts as the offerer, wishes to continue using

the existing association:

```
m=application 54321 SCTP *
c=IN IP4 192.0.2.1
a=setup:passive
a=connection:new
```

Figure 3

The endpoint at 192.0.2.2 also wishes to use the existing Sctp association and responds with the following description:

```
m=application 9 SCTP *
c=IN IP4 192.0.2.2
a=setup:active
a=connection:new
```

Figure 4

The existing Sctp association between 192.0.2.2 and 192.0.2.1 will be reused.

[6.3.](#) SDP description for DTLS Connection

An offerer at 192.0.2.2 signals the availability of a T.38 fax session over Sctp/Dtls.

```
m=image 54111 Sctp/Dtls t38
c=IN IP4 192.0.2.2
a=setup:actpass
a=connection:new
a=fingerprint:SHA-1 \
  4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
```

Figure 5

7. Network Address Translators (NAT) Considerations

SCTP specific features (not present in UDP/TCP), as the checksum (CRC32c) value calculated on the whole packet (not just the header) or multihoming, present new challenges for a NAT.

[[I-D.ietf-behave-sctpnat](#)] describes an SCTP specific variant of NAT which provides similar features of Network Address and Port Translation (NAPT).

As an alternative to design SCTP specific NAT, SCTP-over-UDP [[I-D.tuexen-sctp-udp-encaps](#)] makes possible, encapsulating SCTP packets into UDP packets, to use SCTP in networks with legacy NAT and firewalls not supporting SCTP.

OPEN ISSUE: do we want to include in SDP the ability to signal SCTP-over-UDP ?

TBD: How to use Interactive Connectivity Establishment (ICE) to establish SCTP streams.

OPEN ISSUE: Do we want ICE to only use SCTP over IP candidates, or we want ICE to use SCTP over UDP candidates as well?

8. Security Considerations

See [RFC 4566](#) [[RFC4566](#)] for security considerations on the use of SDP in general. See [RFC 3264](#) [[RFC3264](#)], [RFC 4145](#) [[RFC4145](#)] and [RFC 4572](#) [[RFC4572](#)] for security considerations on establishing media streams using offer/answer exchanges. See [RFC 4960](#) [[RFC4960](#)] for security considerations on SCTP in general and [[RFC6083](#)] for security consideration using DTLS on top of SCTP. This specification does not introduce any new security consideration in addition to the ones discussed in those specifications.

9. IANA Considerations

This document defines two new proto values: 'SCTP' and 'SCTP/DTLS'. Their formats are defined in [Section 3](#). These proto values should be registered by the IANA under "Session Description Protocol (SDP) Parameters" under "proto".

The SDP specification, [[RFC4566](#)], states that specifications defining new proto values, like the SCTP and SCTP/DTLS proto values defined in this RFC, must define the rules by which their media format (fmt) namespace is managed. For the SCTP protocol, new formats SHOULD have an associated MIME registration. 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 [[RFC4288](#)] [[RFC4289](#)] by production of, or reference to, a standards-track RFC that defines the transport protocol for the format.

10. 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.
- [RFC3436] Jungmaier, A., Rescorla, E., and M. Tuexen, "Transport Layer Security over Stream Control Transmission Protocol", [RFC 3436](#), December 2002.
- [RFC4145] Yon, D. and G. Camarillo, "TCP-Based Media Transport in the Session Description Protocol (SDP)", [RFC 4145](#), September 2005.
- [RFC4288] Freed, N. and J. Klensin, "Media Type Specifications and Registration Procedures", [BCP 13](#), [RFC 4288](#), December 2005.
- [RFC4289] Freed, N. and J. Klensin, "Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures", [BCP 13](#), [RFC 4289](#), December 2005.
- [RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", [RFC 4347](#), April 2006.
- [RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", [RFC 4566](#), 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.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), August 2008.
- [RFC6083] Tuexen, M., Seggelmann, R., and E. Rescorla, "Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)", [RFC 6083](#), January 2011.
- [I-D.ietf-behave-sctpnat]
Stewart, R., Tuexen, M., and I. Ruengeler, "Stream Control Transmission Protocol (SCTP) Network Address Translation", [draft-ietf-behave-sctpnat-04](#) (work in progress), December 2010.
- [I-D.tuexen-sctp-udp-encaps]
Tuexen, M. and R. Stewart, "UDP Encapsulation of SCTP Packets", [draft-tuexen-sctp-udp-encaps-06](#) (work in progress), January 2011.

Authors' Addresses

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

