MMUSIC
Internet-Draft
Intended status: Standards Track
Expires: September 10, 2009

S. Loreto
G. Camarillo
Ericsson

March 9, 2009

# Stream Control Transmission Protocol (SCTP)-Based Media Transport in the Session Description Protocol (SDP)

draft-loreto-mmusic-sctp-sdp-03

## Status of this Memo



## Copyright Notice



## 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/TLS' protocol identifiers for SDP.

Table of Contents

## 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 streams. RFC 4572 [RFC4572] extends RFC4145 [RFC4145] for describing TCP-based media streams that are protected using TLS [RFC4346].

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.

Additionaly this document define a new protocol identifier, 'SCTP/TLS', to establish secure SCTP-based media streams over Transport Layer Security (TLS) [RFC3436] using the Session Description Protocol (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].
[I-D.ietf-tsvwg-dtls-for-sctp]

## 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/TLS'.

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/TLS' protocol identifier indicates that the media described will use the Transport Laryer Secturity protocol [RFC4346] over SCTP as specified in RFC3436 [RFC3436].

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

## 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.

OPEN ISSUE: that intermediaries such as SBCs will not be aware of some of the IP addresses used for media because they will not appear in the SDP. We can RECOMMEND that SCTP endpoints use a main address all the time (e.g., not to retransmit to a backup address) and that they send a re-INVITE every time they change that address. Alternatively (or additionally), we could add SDP attributes with all the IP addresses that can be used by the association.

## 6. Examples

The following examples show the use of the 'setup' and 'connection' SDP attributes. As discussed in Section 4, the use of this 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
```

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
```

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 1

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 2

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

### 6.3. SDP description for TLS Connection

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

```
m=image 54111 SCTP/TLS 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
```

## 7. 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 RFC 3436 [RFC3436] for security consideration using TLS on top of SCTP. This specification does not introduce any new security consideration in addition to the ones discussed in those specifications.

## 8. IANA Considerations

This document defines a new proto value: SCTP. Its format is defined in Section 3. This proto value 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/TLS 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 [RFC2048] by production of, or reference to, a standards-track RFC that defines the transport protocol for the format.

## 9. Normative References

[RFC2048] Freed, N., Klensin, J., and J. Postel, "Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures", BCP 13, RFC 2048, November 1996.

[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.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[RFC3436] Jungmaier, A., Rescorla, E., and M. Tuexen, "Transport Layer Security over Stream Control Transmission Protocol", RFC 3436, December 2002.

[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.

[I-D.ietf-tsvwg-dtls-for-sctp] Tuexen, M., Seggelmann, R., and E. Rescorla, "Datagram Transport Layer Security for Stream Control Transmission Protocol", draft-ietf-tsvwg-dtls-for-sctp-00 (work in progress), October 2008.

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