Ideas for a Next Generation of the Stream Control Transmission Protocol (SCTP)
draft-dreibholz-tsvwg-sctp-nextgen-ideas-10

Abstract
This document collects some ideas for a next generation of the Stream Control Transmission Protocol (SCTP) for further discussion. It is a result of lessons learned from more than one decade of SCTP deployment.

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 https://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 March 13, 2020.

Copyright Notice
Copyright (c) 2019 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 (https://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 ........................................ 2
   1.1.  Abbreviations .................................. 2
   1.2.  Stream Control Transmission Protocol ............ 2
   1.3.  Scope ........................................... 2
2.  What to Change in the Next Generation of SCTP? ....... 2
   2.1.  Security Considerations ......................... 3
   2.2.  IANA Considerations ............................. 3
3.  Experimental Implementations ........................... 3
4.  Testbed Platform ...................................... 4
5.  Acknowledgments ....................................... 4
6.  References ........................................... 4
   6.1.  Normative References ............................. 4
   6.2.  Informative References ........................... 6
Author’s Address ........................................ 8

1.  Introduction

1.1.  Abbreviations

   o SCTP: Stream Control Transmission Protocol

1.2.  Stream Control Transmission Protocol

   The Stream Control Transmission Protocol (SCTP) has been defined as
   RFCs in [1], [2], [3], [4], [5], [6], [7], [8], [10], [11], [12],
   [13], [14], [15]. There is also a detailed introduction provided by
   [22] as well as lots of further information material on [19]. SCTP
   is therefore not introduced in more detail here.

1.3.  Scope

   The scope of this document is to collect some ideas of what to
   update/change for a next generation of the SCTP protocol. It is a
   result of lessons learned from more than one decade of SCTP
   deployment (see also [22]) as well as ongoing discussions on applying
   SCTP for WebRTC Data Channels (as introduced in more detail in [18]).

2.  What to Change in the Next Generation of SCTP?

   o Make useful extensions part of the next generation core protocol
     itself (that is, make their implementation a MUST):

     * Partial Reliability ([4])

     * Chunk Authentication ([6])
* Partial Reliability ([8])
* Stream Reconfiguration ([13])
* SACK Immediately ([15])

- Consider additional features as part of the next generation core protocol:
  * Non-Renegable Selective Acknowledgments (NR-SACK) ([24])
  * Concurrent Multi-Path Transfer for SCTP (CMT-SCTP) ([16])

- Chunk Authentication provides integrity but not confidentiality. There could be a feature for encryption as well, for example like [17]. Having encryption directly included inside the core transport protocol may make it easier to use (less error-prone work for application developers).

- SCTP assigns a fixed TSN per DATA chunk. The TSN cannot be changed any more. That is, it is not possible for a middlebox to split chunks into smaller pieces (for example, for hardware offloading). For further discussion: may it be useful to consider a different behavior?

- Definition of path: For SCTP, a path is defined by a remote destination address. [20], [21] shows that CMT-SCTP performance also depends on the local endpoint’s outgoing links. Considering each pair of local outgoing and remote incoming address as different path may lead to improved performance in many Internet scenarios.

### 2.1. Security Considerations

Security considerations for SCTP can be found in [9].

### 2.2. IANA Considerations

This document introduces no additional considerations for IANA.

### 3. Experimental Implementations

An Open Source simulation model for SCTP is available for OMNeT++ within the INET Framework. See [23] for the Git repository. For documentation on the model, see [25] and [22]. This model can be used to evaluate future ideas for SCTP.
4. Testbed Platform

NorNet is a large-scale and realistic Internet testbed platform with support for multi-homing. A description of and introduction to NorNet is provided in [26], [27], [28], [29]. Further information can be found on the project website [30] at https://www.nntb.no.

5. Acknowledgments

The author would like to thank Martin Becke for discussions and support.

6. References

6.1. Normative References


6.2. Informative References


Author’s Address

Thomas Dreibholz
Simula Metropolitan Centre for Digital Engineering
Pilestredet 52
0167 Oslo, Oslo
Norway

Phone: +47-6782-8200
Fax: +47-6782-8201
Email: dreibh@simula.no
URI: https://www.simula.no/people/dreibh