Abstract

This document describes a simple method of encapsulating SCTP Packets into UDP packets. This makes it possible to use SCTP in networks with legacy NAT not supporting SCTP or implement SCTP on hosts without directly accessing the IP-layer.

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 July 14, 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. Conventions .................................................. 3
3. Architecture .................................................. 3
   3.1. General Considerations ............................... 3
   3.2. Internal EDP Considerations ......................... 4
   3.3. External EDP Considerations ......................... 4
4. Port Number Table ............................................. 4
5. Encapsulating Procedures ..................................... 4
6. Decapsulating Procedures .................................. 5
7. Address Management of SCTP Endpoints .................... 5
8. IANA Considerations ......................................... 5
9. Security Considerations ..................................... 5
10. Acknowledgments ............................................ 5
11. References .................................................. 5
   11.1. Normative References ................................. 5
   11.2. Informative References ............................... 6
Authors’ Addresses ............................................ 6
1. Introduction

This document describes a simple method of encapsulating SCTP packets into UDP packets. SCTP is defined in [RFC4960]. There are two main reasons for this:

- Allow SCTP traffic to pass legacy NATs, which do not provide native SCTP support as specified in [I-D.ietf-behave-sctpnat] and [I-D.stewart-natsupp-tsvwg].
- Allow SCTP to be implemented on hosts which do not provide direct access to the IP-layer. In particular, applications can use their own SCTP implementation if the operating system does not provide one.

2. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Architecture

3.1. General Considerations

The basic architecture is shown in the following figure.

```
+----------------+   +----------------+
| Encapsulating/ |   | Encapsulating/ |
| Decapsulating  | ---| Decapsulating  |-+
|     Point      |   |     Point      |
| SCTP Endpoint  |   | SCTP Endpoint  |
```

On each path there is a pair of encapsulating/decapsulating points (EDPs). When the left SCTP endpoint sends an SCTP packet to the right SCTP endpoint, the first EDP on the path encapsulates the SCTP packet and the second EDP decapsulates it. Between the EDP a UDP
packet is sent which can be processed by legacy NATs. The EDPs on
different paths do not need to be synchronized.

3.2. Internal EDP Considerations
TBD.

3.3. External EDP Considerations
TBD.

4. Port Number Table
Every EDP maintains an encapsulating table (ET) where each row
consists of the following entries:

1. Source Address
2. Source Port
3. Destination Address
4. Destination Port
5. Time Stamp

Please note that the port numbers in the ET are used to build the UDP
header while encapsulating. A row SHOULD be deleted when the time
stamp is older than \( T_1 \) seconds. The default value for \( T_1 \) is 300
seconds.

5. Encapsulating Procedures
When an EDP has to encapsulate an SCTP packet it looks up the source
and destination port number in the row with matching source and
destination addresses of the ET. If no matching row is found, the
IANA registered value 9899 is used for the source and destination
port as the result of the lookup procedure. If a matching row was
found, the time stamp of that row is set to the current time.

The EDP inserts then an UDP header between the IP and SCTP header of
the SCTP packet using the source port and the destination port from
the above lookup procedure. Furthermore the length and the checksum
field of the UDP header have to be set accordingly. Finally the IP
header is updated to indicate that it now encapsulates an UDP packet.
6. Decapsulating Procedures

When an EDT has to decapsulate an SCTP packet, it removes the UDP header from the packet. The IP header is updated to indicate that it now encapsulates an SCTP packet. If the source and destination port numbers are not both equal to 9899, the EDP performs a lookup in the ET to find a row with the source address of the packet being the destination address in the row and the destination address of the packet being the source address in the row. If such a row is found, the port numbers are updated. If no row is found, a new one is created using the addresses and the port numbers from the packet by exchanging the source and destination information. In both cases the time stamp of the row is set to the current time.

7. Address Management of SCTP Endpoints

To allow seamless legacy NAT traversal the SCTP endpoints MUST follow the address management procedures described in [I-D.ietf-behave-sctpnat]

8. IANA Considerations

This document does not require any actions from IANA.

9. Security Considerations

This section is not complete yet.

10. Acknowledgments

The authors wish to thank Irene Ruengeler for her invaluable comments.

11. References

11.1. Normative References


11.2. Informative References

[I-D.ietf-behave-sctpnat]

[I-D.stewart-natsupp-tsvwg]

Authors’ Addresses

Michael Tuexen
Muenster University of Applied Sciences
Stegerwaldstr. 39
48565 Steinfurt
Germany

Email: tuexen@fh-muenster.de

Randall R. Stewart
Huawei
Chapin, SC  29036
USA

Email: randall@lakerest.net