Abstract

This document describes a simple method of encapsulating SCTP Packets. This makes it possible to use SCTP in networks with legacy NAT not supporting SCTP.

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on June 24, 2010.

Copyright Notice

Copyright (c) 2009 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 BSD License.

Table of Contents

1. Introduction ............................................... 3
2. Conventions ................................................. 3
3. Architecture ................................................. 3
4. Port Number Table .......................................... 3
5. Encapsulating procedures ................................. 4
6. Decapsulating procedures ................................. 4
7. IANA Considerations ....................................... 5
8. Security Considerations ................................. 5
9. Acknowledgments ........................................... 5
10. References .................................................. 5

10.1. Normative References ................................. 5
10.2. Informative References ................................. 5

Authors’ Addresses ........................................... 5
1. Introduction

This document describes a simple method of encapsulating SCTP packets. This makes it possible to use SCTP in networks with legacy NAT not supporting SCTP. This described method interworks without any problems with the NAT mechanism described in [I-D.stewart-behave-sctpnat]. For general NAT considerations regarding SCTP see [I-D.xie-behave-sctp-nat-cons].

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

The basic architecture is shown in the following figure.

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

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.

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 T1 seconds. The default value for T1 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. IANA Considerations

This document does not require any actions from IANA.

8. Security Considerations

This section is not complete yet.

9. Acknowledgments

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

10. References

10.1. Normative References


10.2. Informative References

[I-D.xie-behave-sctp-nat-cons]
Xie, Q., Stewart, R., Holdrege, M., and M. Tuexen, "SCTP NAT Traversal Considerations",

[I-D.stewart-behave-sctpnat]
Authors’ Addresses

Michael Tuexen  
Muenster Univ. of Applied Sciences  
Stegerwaldstr. 39  
48565 Steinfurt  
Germany  
Email: tuexen@fh-muenster.de

Randall R. Stewart  
Huawei  
Chapin, SC  29036  
USA  
Email: rstewart@huawei.com