Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 26, 2007

M. Tuexen
Muenster Univ. of Applied Sciences
R. Stewart
Cisco Systems, Inc.
November 22, 2006

UDP Encapsulation of SCTP Packets
draft-tuexen-sctp-udp-encaps-01.txt

Status of this Memo

Copyright Notice

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.

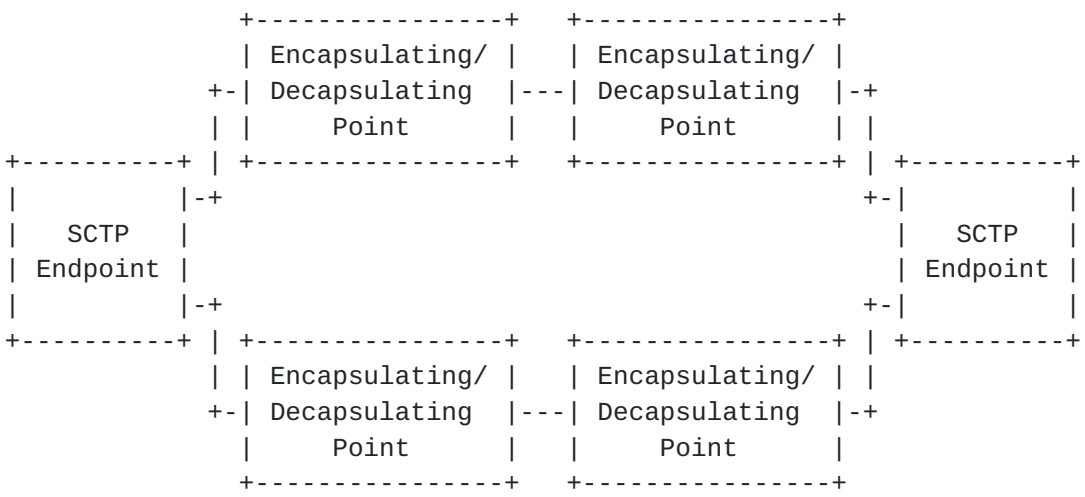
Table of Contents

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 SCTP_NAT [3]. For general NAT considerations regarding SCTP see SCTP_NAT_CONS [2].

2 Architecture

The basic architecture is shown in the following figure.



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 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.

4 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.

5 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.

6 IANA Considerations

This document does not require any actions from IANA.

7 Security Considerations

This section is not complete yet.

8 Acknowledgments

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

9. References

9.1. Normative References

[1] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L., and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

9.2. Informative References

[2] Xie, Q., "SCTP NAT Traversal Considerations", draft-xie-behave-sctp-nat-cons-01 (work in progress), October 2005.

[3] Stewart, R. and M. Tuexen, "Stream Control Transmission Protocol (SCTP) Network Address Translation", draft-stewart-behave-sctpnat-02 (work in progress), May 2006.

Authors' Addresses

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

Email: tuexen@fh-muenster.de

Randall R. Stewart
Cisco Systems, Inc.
4875 Forest Drive
Suite 200
Columbia, SC 29206
USA

Email: rrs@cisco.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).