STREAM CONTROL TRANSMISSION PROTOCOL

Author G.Bhagyasree
CSE, I/II, M.Tech K.L.University
Email: bsri637@gmail.com

ABSTRACT: SCTP is the next generation of the Transmission Control Protocol (TCP). Nowadays, there are SCTP implementations for all major operating systems. While SCTP was standardized as an RFC several years ago, there is still significant ongoing work within the IETF to discuss and standardize further features in the form of protocol extensions. In this article, we first introduce the SCTP base protocol and already standardized extensions. After that, we focus on the ongoing SCTP standardization progress in the IETF and give an overview of activities and challenges in the areas of security and concurrent multipath transport.

INTRODUCTION

In computer networking, the **Stream Control Transmission Protocol** (**SCTP**) is a transport layer protocol, serving in a similar role to the popular protocols Transmission (TCP) and User Datagram Protocol (UDP). It provides some of the same service features of both: it is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP. SCTP is the next generation of the Transmission Control Protocol (TCP). SCTP is a general-purpose transport protocol, which provides the same service as TCP plus a set of advanced features regarding security, multihoming, multistreaming, mobility, and partial reliability. This paper introduces SCTP and gives an overview of recent and ongoing IETF standardization activities for SCTP and its extensions.

BASIC FEATURES

Features of SCTP include:

- Multihoming support in which one or both endpoints of a connection can consist of more than one IP address, enabling transparent fail-over between redundant network paths.
- Delivery of chunks within independent streams eliminates unnecessary head-of-line blocking, as opposed to TCP byte-stream delivery.
- Path selection and monitoring select a primary data transmission path and test the connectivity of the transmission path.
- Validation and acknowledgment mechanisms protect against flooding attacks and provide notification of duplicated or missing data chunks.
- Improved error detection suitable for Ethernet jumbo frames.

1.1 MULTIHOMING

Multi-Homing refers to the ability of utilize multiple addresses for the same host in a network environment. In the case of an IP network, it is possible that one host owns two or more distinct public IP addresses from the same or distinct service providers, in the same way one can own two distinct telephone numbers (i.e., home phone, cell phone, and fax numbers) in PSTN. SCTP uses its multi-homing nature to provide

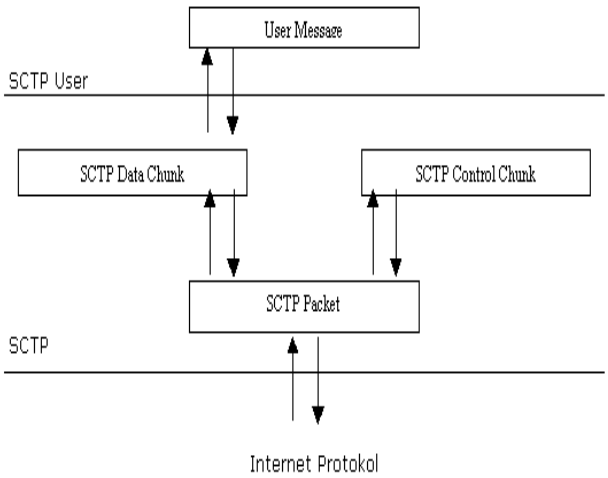
redundancy to the transport layer. During the association establishment, both end points will select one IP address from their pool of addresses and will designate this one as the"primary" path. The remaining pool is utilized as backup in case the connectivity of this primary path fails (a fail is dynamically detected using the special control message HEARTBEAT). Moreover, each end point will exchange their pool of IP addresses in order to let the other end know where this end point can be reached at aside from the primary advertised path. However, an important clarification about multi-homing is the following: SCTP does not do load sharing and multi-homing is used for redundancy purposes only.

1.2 MULTI-STREAMING

In the SCTP context, multi-streaming refers to the parallel transmission of user data over the same association made between two end nodes. In TCP, during the transmission of segments between the two end points, it is possible that the protocol wastes its bandwidth due to the strict sequence of message delivery and thus decreases its cumulative throughput due to network failures. This problem is known as head-of-the-queue blocking. In SCTP, if a stream starts to fail due to message loss or network path failure, only this failing stream will block the delivery of its own sequential packets, while the remaining streams will continue to operate normally. SCTP provides in-sequence delivery for messages within each stream, but not across different streams. If a message of a particular stream is lost, messages of the other streams do not need to be delayed at the receiver until the lost message has been retransmitted and finally received. Therefore, multiple streams can be used to minimize so-called head-of-line blocking. Multiple DATA-chunks containing messages from the same or different streams can be bundled into a single packet.

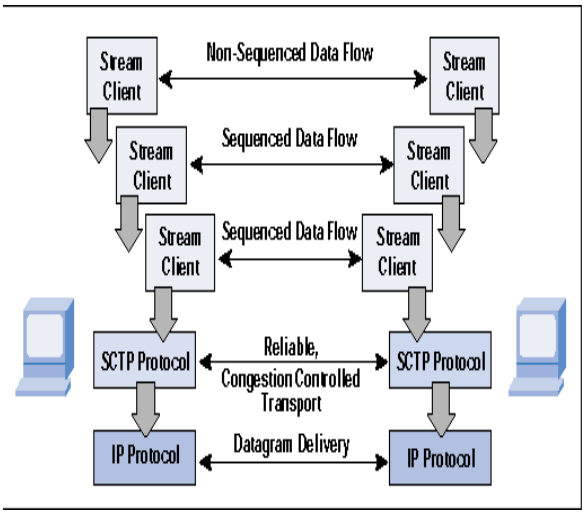
2. SCTP ARCHITECTURE

SCTP is defined to be a transport layer protocol it sits in between the network layer and the upper layers that we will call application for short. User data is taken from the upper layers and received data is reassembled and returned to the user applications expecting this data. Inside the transport layer, the data is fragmented and sequenced before it is sent to the lower layers for its delivery. The received data from the lower layers is checked reassembled and checked for validation before it is delivered to the upper layers.



2.1 PACKET STRUCTURE

Each SCTP packet contains both data and control chunks. The common header section includes information such as the source and destination port numbers to associate it with the application it belongs, the verification tag introduced before, and the checksum to test the integrity of the packet. The first chunks can be either control or data chunks (due to early start of data transfer during the initialization phase), but consecutive chunks are data. Finally, the number of chunks in a SCTP packet is determined during the initialization of the association in order to cooperate state during the initialization.



2.2 CHUNKS

The chunk is the minimal data unit that can be transmitted in SCTP. Contrary to TCP that transmits bytes, chunks in SCTP can be used to control the association between nodes, test the validity of the announce paths, and provide mechanisms for diverse network events, such as failure, disconnection, or abort (half-open connections).

2.3 INITIALIZATION PHASE

A connection in SCTP is termed"association," and it is much more than the simple three-way hand-shake in TCP. SCTP uses a four-way hand-shake mechanism that seeks to eliminate the SYN in TCP that can initiate a ultimate result in the Denial of Service on the host. A cookie mechanism is used to achieve this purpose. For illustrative purposes, the connecting end will be called A, and the receiving connection will be called B from now on.

2.4 GRACEFUL TERMINATION

SCTP provides graceful termination in all its associations made. However, there are occasions when this is not achieved. For example, TCP supports half-open nodes with no problem, but this is not the case of SCTP. In the event an association is not terminated appropriately, ABORT messages are used to cleanly terminate the rest of the association that stills alive. On the other hand, we have the normal termination of an association that is started with SHUTDOWN messages.

3. WHO SUPPORTS SCTP

SS7-Signal System 7- In the earliest days of telephony, if one wanted to make phone calls, they bought a pair of handsets connect by a wire, and they laid that wire between themselves and someone that they intended

to have conversations with. To initiate a call, they could yell into their handset and hope the person on the other end would hear them through their handset and pick up. Calls between another third party and the handset owner would require a second set of handsets connected by a wire. Three way calling was nonexistent. Enter the telephone company. Now there were centralized switchboards where a caller need only connect to the centralized hub and a call could be set up by allotting a circuit to two individuals who needed to talk to one another. Eventually dialing of numbers was introduced, under which numbers of clicks (interruptions) on the line allowed the user to directly dial the number they wished to call. These clicks were signals that allowed one to set-up a call. Enter the digital age. Phone companies realizing that they would be wasting valuable resources trying to accommodate high voice traffic began using a separate digital line to transfer all of the signaling for calls. SS7 is the standardization of the digital signaling network phone companies use. It is the only network that currently supports SCTP.

4. SCTP GENERAL FEATURES

• Equivalent level as TCP and UDP

• Reliable transport service

• Error-free

• In sequence

• Session-oriented mechanism

5. PERFORMANCE EVALUATION

Single File Transfer

• Compare latency of file transfer using TCP and SCTP for files of different sizes

• Compare latency in packet-loss environment for varying loss percentages

Multiple File Transfer

• Compare latency and throughput in transferring multiple files for varying number of files

• Compare latency and throughput in packet-loss environment for varying loss percentages

6. ADVANTAGES

- **Four-way Hand-shake**: One of the most noticeable problems found in TCP is its vulnerability to Denial of Service attacks (DoS), also known as blind attacks. SCTP provides a mechanism to authenticate the initiator of an association with the server by the use of a cookie mechanism in a four-way hand-shake. By sending a challenge to the requester of the communication, the server will not allocate any resources at this point, but effectively will transmit information that is necessary to establish the association.
- **Parallel association integration**: Parallel association refers to the attempt of a node to establish more than one association with the same node. This is possible since the

protocol assumes. For this reason SCTP is a multi-stream protocol, and uses these streams to handle the multiple connections.

- **Multi-streams**: Introduced in the previous paragraph, the use of multi-streams is one of the best additions of SCTP to the transport layer. SCTP has not that type of sequencing since it uses multiple streams to transmit data to the requester. Because these streams are independent, and because SCTP is a message-oriented protocol, SCTP has a comparative advantage over TCP by resolving the issue of packet loss. If a stream stops transmitting data due to network problems, the other streams will not be obstructed by this stream and will continue to deliver messages without any problems. An important observation is the following. Overall, it is expected that SCTP improves its throughput compared with the one obtained in TCP.
- **Redundancy:** SCTP provides redundancy by the use making the end nodes multi-homing.
- **Reachability Monitoring**: SCTP provides for the support for continuous monitoring of reachability. Through the mechanism of the heartbeat chunk, connectivity is constantly checked to determine whether or not a particular IP to IP connection is available.
- **Notorious Network Failures**: This continuous monitoring of reachability is a hallmark of SCTP and nonexistent in the TCP protocol.
- **Security**: Although encryption was not part of the original SCTP design, SCTP was designed with features for improved security, such as 4-way handshake (compared to TCP 3-way handshake) to protect against SYN flooding attacks, and large "cookies" for association verification and authenticity.

7. CONCLUSION

In this paper, we have given an overview of the recent advances in the IETF standardization process of the SCTP protocol and its extensions. While the core SCTP protocol, including the extensions for partial reliability, chunk authentication, and dynamic address reconfiguration, already completed standardization within the IETF SIGTRAN WG and TSVWG some time ago, there is still a significant amount of ongoing work within the TSVWG and BEHAVE WG to standardize further enhancements like SACK immediately, stream reset, the socket API, and an SCTP-aware NAT. Also, there is clear interest in CMT with SCTP, which is currently under development by multiple research groups and is expected to dominate SCTP standardization activities in the coming years.

References:

R. Sengelmann, M. Tüxen, and E. P. Rathgeb, “Design and Implementation of SCTP-aware DTLS,” Proc. Int’l. Conf. Telecommun. And Multimedia, July 2010.

J. R. Iyengar, P. D. Amer, and R. Stewart, "Concurrent Multipath Transfer Using to-End Paths," IEEE/ACM Trans. Net., vol. 14, no 5, Oct. 2006, pp. 951–64.

R. Stewart et al., "Stream Control Transmission Protocol (SCTP) Partial Reliability Extension," IETF RFC 3758, May 2004.

M. Tüxen et al., "Authenticated Chunks for the Stream Control Transmission Protocol (SCTP)," IETF RFC 4895, Aug. 2007.

SCTP Multihoming over Independent End-

R. Stewart. Stream Control Transmission Protocol. RFC 4960, September 2007.

R. Stewart, M. Tüxen, and I. Rüngeler, "Stream Control Transmission Protocol (SCTP) Network Address Translation," draft-ietf-behave-sctpnat-04.txt, Dec. 2010.

M. Tüxen, R. Seggelmann, and E. Rescorla, "Datagram Transport Layer Security for Stream Control Transmission Protocol," IETF RFC 6083, Jan. 2011.

