Delay-Tolerant Networking Working Group
Internet Draft
Intended status: Standards Track
Expires: March 2019

S. Burleigh
JPL, Calif. Inst. Of Technology

September 14, 2018

Simple TCP Convergence-Layer Protocol
draft-burleigh-dtn-stcp-00.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a Simple TCP (STCP) "convergence-layer" protocol for the Delay-Tolerant Networking (DTN) Bundle Protocol (BP). STCP uses Transmission Control Protocol (TCP) to transmit BP "bundles" from one BP node to another node to which it is topologically adjacent in the BP network. The services provided by the STCP convergence-layer protocol adapter utilize a standard TCP connection for the purposes of bundle transmission.

Table of Contents

1. Introduction

This document describes the Simple TCP (STCP) protocol, a Delay-Tolerant Networking (DTN) Bundle Protocol (BP) [RFC5050] "convergence layer" protocol that uses a standard TCP connection to transmit bundles from one BP node to another node to which it is topologically adjacent in the BP network.

Conformance to the STCP convergence-layer protocol specification is OPTIONAL for BP nodes.

Each BP node that conforms to the STCP specification includes an STCP convergence-layer adapter (SCLA). Every SCLA engages in communication via the Transmission Control Protocol [RFC0793].

Like any convergence-layer adapter, the STCP CLA provides:

- A transmission service that sends an outbound bundle (from the bundle protocol agent) to a peer CLA via the STCP convergence layer protocol.
- A reception service that delivers to the bundle protocol agent an inbound bundle that was sent by a peer CLA via the STCP convergence layer protocol.

Transmission of bundles via STCP is "reliable" to the extent that TCP itself is reliable. STCP provides no supplementary error detection and recovery procedures. In particular, STCP does not provide to the sender any intermediate reporting of reception progress.

2. Conventions used in this document

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 RFC-2119 [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

3. STCP Design Elements

3.1. STCP Sessions

An STCP "session" is formed when a TCP connection is established by the matching of an active TCP OPEN request issued by some SCLA, termed the session's "sender", with a passive TCP OPEN request issued by some SCLA, termed the session's "receiver". That portion of the state of a session that is exposed to the session's sender is termed the "transmission element" of the session. That portion of the state of a session that is exposed to the session's receiver is termed the "reception element" of the session.

The values of the parameters constraining STCP's TCP connection establishment, including the establishment of Transport Layer Security (TLS; [RFC8446]) sessions within the connections, are assumed to be provided by management. At some point a discovery protocol may be developed that enables these values to be declared

automatically; such protocol is beyond the scope of this specification.

STCP sessions are unidirectional; that is, bundles transmitted via an STCP session are transmitted only from the session's sender to its receiver. When bidirectional exchange of bundles between SCLAs via STCP is required, two sessions are formed, one in each direction.

Closure of either element of a session MAY occur either upon request of the bundle protocol agent or upon detection of any error. Closure of either element of an STCP session SHALL cause the corresponding TCP connection to be terminated (unless termination of that connection was in fact the cause of the closure of that session element). Since termination of the associated TCP connection will result in errors at the other element of the session, termination of either element of the session will effectively terminate the session.

3.2. STCP Protocol Data Units

An STCP protocol data unit (SPDU) is simply a serialized bundle preceded by an integer indicating the length of that serialized bundle. An SPDU is constructed as follows.

Each SPDU SHALL be represented as a CBOR array. The number of items in the array SHALL be 2.

The first item of the SPDU array SHALL be the length of the serialized bundle that is encapsulated in the SPDU, represented as a CBOR unsigned integer.

The second item of the SPDU array SHALL be a single serialized BP bundle, termed the "encapsulated bundle", represented as a CBOR byte string.

4. STCP Procedures

4.1. SPDU Transmission

When an SCLA is requested by the bundle protocol agent to send a bundle to a peer SCLA identified by some IP address and port number:

. If no STCP session enabling transmission to that SCLA has been formed, the SCLA SHALL attempt to form that session. If this attempt is unsuccessful, the SCLA SHALL inform the bundle protocol agent that its data sending procedures with regard to

this bundle have concluded and transmission of the bundle was unsuccessful; no further steps of this procedure will be attempted.

. The SCLA SHALL form an SPDU from the subject bundle.
. The SCLA SHALL attempt to send this SPDU to the peer SCLA by TCP via the transmission element of the session formed for this purpose.
  o If that transmission is completed without error, the SCLA SHALL inform the bundle protocol agent that its data sending procedures with regard to this bundle have concluded and transmission of the bundle was successful.
  o Otherwise:
    . The transmission element SHALL be closed.
    . The SCLA SHALL inform the bundle protocol agent that its data sending procedures with regard to this bundle have concluded and transmission of the bundle was unsuccessful.

4.2. Reception Session Formation

An SCLA that is required to receive (rather than only transmit) bundles SHALL issue a passive TCP OPEN. Whenever TCP matches that passive OPEN with an active TCP OPEN issued by some SCLA, an STCP session is formed as noted earlier; SPDUs may be received via the reception element of such session.

4.3. SPDU Reception

From the moment at which an STCP session reception element is first exposed to the moment at which it is closed, in a continuous cycle, the corresponding session's receiver SHALL:

. Attempt to receive, by TCP via the corresponding session, the length of the next bundle sent via this session. If this attempt fails for any reason, the reception element SHALL be closed and no further steps of this procedure will be attempted.
. Attempt to receive, by TCP via the corresponding session, a serialized bundle of the indicated length. If this attempt fails for any reason, the reception element SHALL be closed and no further steps of this procedure will be attempted.
. Deliver the received serialized bundle to the bundle protocol agent.

5. Security Considerations

Because STCP constitutes a nearly negligible extension of TCP, it introduces virtually no security considerations beyond the well-known TCP security considerations.

An adversary could mount a denial-of-service attack by repeatedly establishing and terminating STCP sessions; well-understood DOS attack mitigations would apply.

Maliciously formed bundle lengths could disrupt the operation of STCP session receivers, but STCP implementations need to be robust against incorrect bundle lengths in any case.

Maliciously crafted serialized bundles could be received and delivered to the bundle protocol agent, but that is not an STCP-specific security consideration: all bundles delivered to the BPA by all convergence-layer adapters need to be processed in awareness of this possibility.

6. IANA Considerations

No new IANA considerations apply.

7. References

7.1. Normative References

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, August 2018.

7.2. Informative References

[RFC5050] Scott, M. and S. Burleigh, "Bundle Protocol Specification", RFC 5050, November 2007.

8. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Appendix A. For More Information

Please refer comments to dtn@ietf.org. The Delay Tolerant Networking Research Group (DTNRG) Web site is located at http://www.dtnrg.org.

Authors' Address

Scott Burleigh
Jet Propulsion Laboratory, California Institute of Technology
4800 Oak Grove Dr.
Pasadena, CA 91109-8099
US
Phone: +1 818 393 3353
Email: Scott.Burleigh@jpl.nasa.gov