Stream: Independent Submission
RFC: 9401
Category: Informational
Published: 1 April 2023
ISSN: 2070-1721
Author: S. Toyosawa
Independent

RFC 9401
The Addition of the Death (DTH) Flag to TCP

Abstract

This memo specifies the incorporation of Death (DTH) flag to TCP, including DTH's use of one bit in the TCP header. The flag is designed to make TCP session narratives smooth and attractive.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9401.

Table of Contents

1. Introduction

The proposed Death flag, or DTH for short, uses the fourth flag bit in the TCP header to indicate likely termination of the TCP session.

The flag allows applications to prepare for abrupt session terminations. Network engineers find this feature helpful in identifying the one or more root causes of TCP RSTs. Critical end users can use the information to better understand TCP narratives.

The flag name is adapted from the custom of anime, manga, or light novels [NOVEL]. "Death Flags" refer to hints that a character will die soon [CBR-FLAG].

For example, the DTH flag of an evil scientist is set when they express too much confidence in their deadly invention. The scientist is often killed by their own invention. This type of narrative is also common in conventional films. A notable example is a solider in a trench. The soldier's flag is set to 1 immediately after they share a photograph of their fiancé and tell about the upcoming marriage that will take place after returning from battle. Another example is setting the flag for a couple sneaking out from an isolated cabin for a late-night excursion. Commonly, the excursion is violently terminated by an individual with a chainsaw.

2. Requirements Language

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Specification

3.1. TCP Packet Format

The DTH flag uses the fourth bit in the Control bits field in TCP header as depicted in Figure 1 [RFC9293]. The fourth bit was intentionally selected because "four" in Chinese is Sì; it has a similar sound to Sǐ, which means "die".

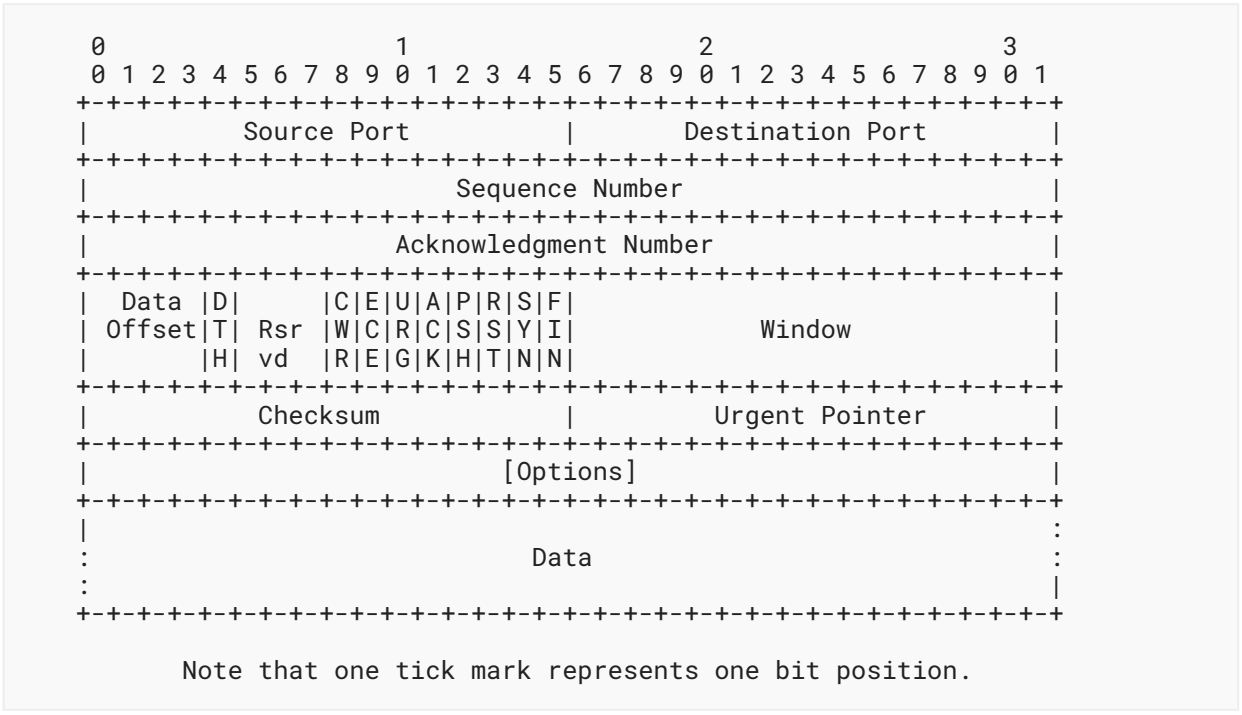

Figure 1: TCP Header with the DTH Flag Bit

A TCP session peer **SHOULD** transmit a DTH segment when the TCP session will likely be terminated soon. It can be sent from both the server and client. The application or TCP stack **MAY** elect not to send DTH segments, even if it knows that the session will be terminated. This results in a dramatic surprise for the peer; however, the end users may perceive the end too convenient

or overly simplistic. Use of the DTH segment that is not associated with the session termination is not encouraged but it is permitted. (This is often referred to as "teasing" or a false-positive DTH flag.)

The DTH flag is informational. TCP software that does not implement this feature can safely ignore this flag. However, to fully appreciate the session, users should be aware of the subtle signs of the session narratives.

The DTH flag itself does not change the sequence or acknowledgment number. It does not require any acknowledgement.

The recipient of the flag is not required to act differently upon reception; however, it is **RECOMMENDED** that information be conveyed to the application layer, so the end user can be notified of the incident. The recipient of a DTH segment **SHOULD NOT** close the socket immediately upon reception; it **SHOULD** wait for a RST or FIN segment.

This specification does not stipulate the maximum number of DTH segments permitted in one TCP session; however, limiting them to a few is **RECOMMENDED** to maximize the dramatic effect.

3.2. When to Send

DTH can be used any time the sender considers it important to signal its inevitable end to the TCP peer. The example scenarios below illustrate when to send DTH segments.

A malicious actor can send the flag when it suddenly repents; for example, when a sender suddenly regrets their part in a DDoS attack and unexpectedly ceases the attack. The archvillain generally terminates the sender cruelly and mercilessly soon after the change in behavior (or they are killed for protecting the hero). The timing of DTH transmission is implementation dependent. It can be sent anytime from the early signs of betrayal to just prior to the behavioral change.

The flag can be sent when the sender stops using cryptographic protections and reveals its plain-text content, for example, a mysterious character with a mask that often dies after they expose their face. In this example, the DTH segment would be sent just before sending the redirect (30x) from HTTPS to HTTP [RFC9110]. Similarly, the flag can be set when the forged User-Agent or Server HTTP header field is changed to the actual value, when their true identity would be revealed (for example, "I am your long-lost twin", "I am a spy", etc.). This occasionally leads to the death of the character.

The TCP peer is **RECOMMENDED** to send the flag when it notices resource issues, e.g., diminishing memory space or bandwidth. An AI bot, cyborg, sorcerer application with forbidden protocols, etc., **SHOULD** consider sending the flag when it starts to heavily cough error messages.

An application less capable of performing its task **MAY** send the flag from time to time. It will be killed by the OS (the archvillain) or CTRL-C (the end user) sooner or later due to its inefficiency. The same is likely to occur with a memory-hogging application, for example, an unscrupulous character that attempts to take all the treasure often dies accidentally (e.g., falls from a cliff).

An application **SHOULD** really think twice before accessing a "honeypot" or haunted server. If your choices are limited (e.g., your favorite server breaks down in the middle of nowhere and the dark server that is not on the DNS is the only place you can shelter), sending the flag periodically is a good idea. The session is most likely cursed.

3.3. When Not to Send

The DTH flag **SHOULD NOT** be piggybacked on the FIN flag. If present, the recipient **SHOULD** silently ignore DTH flag. The only exception is when the recipient is an expert at Hokuto-Shinken ("Big Dipper Divine Fist") [WIKI-FNS]. In that circumstance, the sender is already dead but remains active for a few seconds (which is unofficially called the "half-zombie open" state).

The DTH flag **SHOULD NOT** be sent with the URG flag [RFC6093]. The use of the URG flag is not recommended in new implementations [RFC9293].

Use of the flag in the early state of a TCP session is **NOT RECOMMENDED**. Characters that die in the early stage are considered nonessential, hence their death does not contribute to the quality of the session. (Obviously, there are exceptions.)

3.4. Use with the IP Evil Bit

Some experimental implementations use the Evil bit [RFC3514] of the IP header to indicate if the session portrays an evil character. The DTH flag is not designed to characterize a TCP session. It is intended to show the fate of the session irrespective of the nature of the session. When both Evil bit and DTH flag are present, they **MUST** be interpreted independently.

4. Security Considerations

Precursors to the inevitable death (often violent) of a TCP session are useful for upper-layer applications and end users; however, the security vs. usability balance should also be considered. Since DTH flags may expose the internal state of the TCP session, they can be exploited by attackers (e.g., naming the murderer before the detective points out the suspect). Spoilers are an act of evil. Those who wish to keep the story secret should use the flag mildly.

5. IANA Considerations

This document defines the behavior of the one of the currently reserved (Rsrvd) control bits in the TCP header. It is used as an informative indicator of the fate of a TCP session. The fourth bit (counting from the beginning of the thirteenth octet in a TCP header) is intentionally selected to signify its meaning; however, a change in the bit position does not cause any functional deterioration.

This feature may already be implemented in different manners in Hollywood and/or Japanese animation studio networks; however, to the author's knowledge, the technology is not yet patented.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3514] Bellovin, S., "The Security Flag in the IPv4 Header", RFC 3514, DOI 10.17487/RFC3514, April 2003, <https://www.rfc-editor.org/info/rfc3514>.

[RFC6093] Gont, F. and A. Yourtchenko, "On the Implementation of the TCP Urgent Mechanism", RFC 6093, DOI 10.17487/RFC6093, January 2011, <https://www.rfc-editor.org/info/rfc6093>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9293] Eddy, W., Ed., "Transmission Control Protocol (TCP)", STD 7, RFC 9293, DOI 10.17487/RFC9293, August 2022, <https://www.rfc-editor.org/info/rfc9293>.

6.2. Informative References

[CBR-FLAG] Stalberg, A., "10 Death Flags That Mean An Anime Character is Probably Going To Die", 2023, <https://www.cbr.com/anime-death-hints-signs/>.

[NOVEL] Wikipedia, "Light novel", February 2023, <https://en.wikipedia.org/w/index.php?title=Light_novel&oldid=1136814877>.

[RFC9110] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP Semantics", STD 97, RFC 9110, DOI 10.17487/RFC9110, June 2022, <https://www.rfc-editor.org/info/rfc9110>.

[WIKI-FNS] Wikipedia, "List of Fist of the North Star characters", March 2023, <https://en.wikipedia.org/w/index.php?title=List_of_Fist_of_the_North_Star_characters&oldid=1145633265>.

Author's Address

Satoshi Toyosawa
Independent
Email: s2.toyosawa@gmail.com