Network Working Group
Internet-Draft
Expires: October 13, 2004

L. Eggert
NEC
April 14, 2004

TCP Abort Timeout Option
draft-eggert-tcpm-tcp-abort-timeout-option-00

Status of this Memo

Copyright Notice

Abstract

The TCP Abort Timeout Option allows conforming TCP implementations to negotiate individual, per-connection abort timeouts. Lengthening abort timeouts allows established TCP connections to survive periods of disconnection.

1. Introduction

Some hosts are only intermittently connected to the Internet. One example is mobile hosts that change network attachment points based

on current location, for example using MobileIP [5] or HIP [6]. In between connected periods, mobile hosts may experience disconnected periods during which no network service is available. When such hosts use the Transmission Control Protocol (TCP) [1], their established TCP connections can abort during periods of disconnection.

The TCP specification [1] includes a "user timeout" that defines the maximum amount of time that segments may remain unacknowledged before TCP will abort the connection. If a disconnection lasts longer than the user timeout, the TCP connection will abort. The TCP specification [1] does not constrain the permitted values for user timeouts. Many TCP implementations default to user timeout values of a few minutes [7].

Instead of a single user timeout, some TCP implementations offer finer-grained mechanisms. For example, Solaris supports different timeouts depending on whether a TCP connection is in the SYN-SENT, SYN-RECEIVED, or ESTABLISHED state [8]. (The Host Requirements document [2] requires the timeout to be at least three minutes for the SYN-SENT case.)

This document specifies a new TCP option - the Abort Timeout Option - that allows conforming hosts to negotiate per-connection abort timeouts. This allows mobile hosts to maintain TCP connections across disconnected periods that are longer than their system’s default abort timeout.

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 [3].

2. Specification

Figure 1 shows the format of the TCP Abort Timeout Option. In Figure 1, "X" is a TCP option number to be assigned by IANA upon publication of this document (see Section 5.) "Abort Timeout" is the desired abort timeout of the connection, specified in seconds.

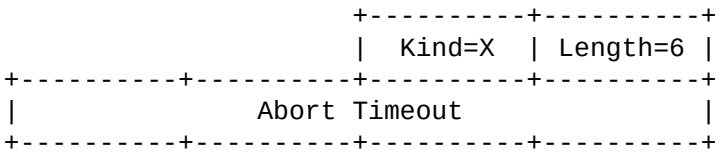

Figure 1: TCP Abort Timeout Option

2.1 Operation

A host wishing to negotiate a specific abort timeout for a connection MAY include the TCP Abort Timeout Option in any segment with a SYN flag, i.e., either the initial SYN or the SYN-ACK. It MUST NOT include an Abort Timeout Option in any other segment.

The timeout value included in the option specifies the proposed abort timeout for the connection. Connections use abort timeouts negotiated with Abort Timeout Options during the ESTABLISHED state only. When connections are in other states, normal timeouts are used [1][2].

A host proposing an abort timeout to its peer MUST be prepared to accept a shorter timeout value than proposed after the negotiation. See Section 2.2 for a discussion of valid timeout values.

Upon receipt of a segment with the Abort Timeout Option, the receiving host decides whether to accept, shorten, or reject its peer's proposed abort timeout. Section 2.3 discusses the specifics of this decision.

When a receiving host accepts or shortens the offered abort timeout, it MUST include an Abort Timeout Option with the corresponding timeout value in the next segment it sends. This will either be the SYN-ACK, if it received the peer's Timeout Abort Option in the SYN segment, or the first ACK if it received the option in the SYN-ACK segment.

This specification allows both the initiator of a TCP connection (i.e., the node sending the SYN) as well as the responder of a TCP connection (i.e., the node receiving the SYN) to initiate an abort timeout negotiation during the connection's three-way handshake. Figure 2 illustrates the two allowed exchanges.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.