MPTCP Working Group
Internet-Draft
Intended status: Informational
Expires: January 9, 2020

V. Tran
O. Bonaventure
Universite catholique de Louvain

July 08, 2019

Multipath TCP Inactivity Time Option
draft-hoang-mptcp-inactivity-time-00

Abstract

This document discusses the lifetime of idle MPTCP sessions, and defines an MPTCP Option subkind for hosts to announce and request this value.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 9, 2020.

Table of Contents

1. Introduction

Multipath TCP [RFC6824] [I-D.ietf-mptcp-rfc6824bis] is used in various use cases [RFC8040]. In several of these deployments, a Multipath TCP connection is composed of a number of subflows that varies during the lifetime of the connection. TCP implementations create state when a connection starts and maintain this state until the abrupt or graceful termination of the connection according to the TCP state machine [RFC0793]. Multipath TCP implementations need to maintain two types of states:

- the per-Multipath TCP connection state that includes the connection keys, data sequence numbers, ...
- the per-TCP subflows connection states

The per-TCP state of each subflow is managed according to [RFC0793]. The Multipath TCP connection state also needs to be managed. We consider a subflow to be active if its TCP state machine exists and is in the Established state. We call inactive a Multipath TCP connection that currently has no active subflow. It is important to note that it is possible for one host to consider a given Multipath TCP connection to be inactive while the other endpoint considers that the connection is still active. This can happen for example when some packets are lost or when one of the hosts has received a spurious RST on the only active subflow. [RFC6824] and [I-D.ietf-mptcp-rfc6824bis] specify how this state can be removed upon transmission or reception of a FASTCLOSE and after having exchanged DATA_FINs. However, [RFC6824] and

[I-D.ietf-mptcp-rfc6824bis] do not specify precisely how the Multipath TCP connection state must be managed when all the TCP subflows associated with this Multipath TCP connection have been released. A similar problem existed in TCP for idle connections. It was clarified in [RFC1122].

Given the cost of maintaining state for inactive Multipath TCP connections, hosts may want to limit the time during which they maintain state for inactive Multipath TCP connections. Neither [RFC6824] nor [I-D.ietf-mptcp-rfc6824bis] propose a default duration to maintain this state. Although some applications such as http/1.1 include a mechanism to terminate idle connections, many applications do not do this. We fill this gap in this document and propose a Multipath TCP option that enables hosts to agree on a common minimum duration to maintain inactive Multipath TCP connections.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

3. Lifetime of Multipath TCP connections

A Multipath TCP connection starts with a three-way-handshake that uses the MP_CAPABLE option and ends with either the transmission of DATA_FINs or a FASTCLOSE. Between these two events, the number of subflows that compose the connection may vary and during some periods of time, it is possible that no active subflow is associated with an existing Multipath TCP connection.

There are several types of events which can occur during the lifetime of a Multipath TCP connection:

- establishment of a new subflow
- graceful termination of subflow with the exchange of FINs
- abrupt termination of a subflow due to multiple expirations of its retransmission timer, the reception of a RST or an abnormal packet, ...

To support the establishment of a new subflow with the MP_JOIN option, a host must maintain state for all established Multipath TCP connection. Neither [RFC6824] nor [I-D.ietf-mptcp-rfc6824bis] specify how a host should behave upon (graceful or abrupt) termination of the last subflow associated with an existing Multipath

TCP connection. One possibility would be to consider that since no subflow is associated with this connection, its state could be freed. A consequence of this policy is that it would then be impossible to establish a new subflow to this connection to recover from the failure of the previous one. Another possibility is to preserve the state of this Multipath TCP connection for some period of time. This would better match the expectations of mobile use cases where subflows can fail abruptly when devices move.

This document proposes the utilisation of an Inactivity timer in Multipath TCP implementations. This timer bounds the time during which there is no active subflow associated with a given Multipath TCP connection. It starts when the last active subflow associated with a connection is terminated. It is reset when one active subflow is associated with this Multipath TCP connection. Upon expiration of this timer, the host SHOULD remove state for the associated Multipath TCP connection. If a host wants to maintain a Multipath TCP connection as active, it SHOULD try to reestablish a subflow associated with this Multipath TCP connection before the expiration of its inactivity timer. This document suggests implementations to start the reestablishment of such a subflow after half the Inactivity timer.

4. The Multipath TCP Inactivity Timer Option

The Multipath TCP Inactivity Timer Option (MPTCP ITO) is used to exchange the Inactivity Timer associated with this connection. This documents recommends a default value of 2 hours and 4 minutes - the same as default NAT timeout as discussed in [RFC5382]. The reason for this value is to allow the peer with default keepalive timer of 2 hours ([RFC1122]) to probe successfully.

4.1. Option Format

The format of the ITO option is depicted in Fig. Figure 1:

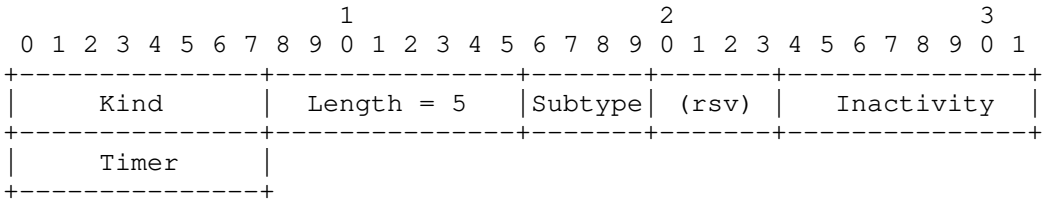

Figure 1: MPTCP Inactivity Timer Option Format

In the ITO option, the Inactivity Timer (16 bits) specifies the requested Timer for the MPTCP session in seconds. A value of zero indicates that the state for the Multipath TCP connection will be removed as soon as there is no active subflow.

4.2. ITO Option and Local Policies

The ITO option is used to specify the value of the Inactivity timer associated with the connection by the host that sends the option. Upon reception of this option, the receiver SHOULD update its ITO option based on the ITO option received from its peer. However, it MAY choose to apply and transmit its own ITO option, depending on its local policies. Note that the ITO option is an indicative value. A host may terminate long inactive connections before the expiration of the ITO timer due to the increasing memory resource pressure.

Like all Multipath TCP options, the ITO Option is exchanged without any protection from TCP's reliability mechanisms. Therefore, implementations MUST NOT assume that it is transferred reliably. Implementations that use the ITO option can transmit the ITO option at any time. Since the utilisation of this option is not negotiated during the connection handshake, a host MUST NOT send more than three ITO options on a connection where it has not received any ITO option.

After the expiration of the Inactivity timer, the host MAY choose to close the MPTCP session with MPTCP_RST and all of its subflows with TCP_RST, and report the inactivity timeout error to the user. This is a common case on the servers that want to free the resource occupied by unused sessions as soon as possible so that they could serve other users.

5. Implementation and Interoperability

5.1. Interaction with TCP Keepalives

The mechanism specified in this document operates above the TCP Keepalives defined in [RFC1122]. If TCP Keepalives are enabled on at least one of the subflows of a Multipath TCP connection, then this subflow will remain active and the Inactivity timer of the associated Multipath TCP connection will not expire. In this case, the Inactivity timer should be longer than the TCP Keepalive timer. If TCP Keepalives are disabled, then the mechanism described in this document will remove the state of the inactive connections.

On some MPTCP implementations like Linux, the TCP Keepalive is supported at the MPTCP layer. To implement the idle timeout option, these implementations may use the MPTCP KeepAliveTime value to keep track of the current idle time. However, the idle timeout mechanism,

when activated, should override the keepalive mechanism. This means that after the idle timeout fired, the host should abort the connection instead of sending the TCP keepalives.

The MPTCP Inactivity Timer Option MAY be controlled on a system-wide setting or on a per-connection basis. Specific APIs and mechanisms for controlling the ITO option are out of the scope of this document.

5.2. Interaction with User Timeout

The interactions between the User Timeout option [RFC5482] and the ITO option will be discussed in a subsequent revision of this document.

6. Security Considerations

The ITO option enables hosts to exchange the value of a timer that protects against some types of ressource exhaustion attacks. Multipath TCP implementations should define a range of safe values for the ITO option and prevent applications from configuring an inactivity timer outside this range. They should also ignore received ITO options that are outside this range.

Since the ITO option is neither encrypted nor authenticated, on-path attackers and middleboxes could remove, add or modify the ITO option on observed Multipath TCP connections.

7. IANA Considerations

IANA is requested to assign an MPTCP option subtype for the ITO option from the "MPTCP Option Subtypes" available at https://www.iana.org/assignments/tcp-parameters/tcp-parameters.xhtml

8. Acknowledgements

This work was supported by the ARC-SDN project and the Walinnov MQUIC project, No. 1810018.

9. References

9.1. 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>.

9.2. Informative References

[I-D.ietf-mptcp-rfc6824bis]
Ford, A., Raiciu, C., Handley, M., Bonaventure, O., and C. Paasch, "TCP Extensions for Multipath Operation with Multiple Addresses", draft-ietf-mptcp-rfc6824bis-18 (work in progress), June 2019.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <https://www.rfc-editor.org/info/rfc793>.

[RFC1122] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <https://www.rfc-editor.org/info/rfc1122>.

[RFC5382] Guha, S., Ed., Biswas, K., Ford, B., Sivakumar, S., and P. Srisuresh, "NAT Behavioral Requirements for TCP", BCP 142, RFC 5382, DOI 10.17487/RFC5382, October 2008, <https://www.rfc-editor.org/info/rfc5382>.

[RFC5482] Eggert, L. and F. Gont, "TCP User Timeout Option", RFC 5482, DOI 10.17487/RFC5482, March 2009, <https://www.rfc-editor.org/info/rfc5482>.

[RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 6824, DOI 10.17487/RFC6824, January 2013, <https://www.rfc-editor.org/info/rfc6824>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

Authors' Addresses

Viet-Hoang Tran
Universite catholique de Louvain

Email: hoang.tran@uclouvain.be

Olivier Bonaventure
Universite catholique de Louvain
Pl. Ste Barbe, 2
Louvain-la-Neuve 1348
Belgium

Email: olivier.bonaventure@uclouvain.be