

Network Working Group
Internet-Draft
Updates: [6824](#) (if approved)
Intended status: Experimental
Expires: January 7, 2016

M. Boucadair
C. Jacquenet
France Telecom
July 6, 2015

Probing MPTCP Subflows
draft-boucadair-mptcp-probe-subflow-00

Abstract

This document specifies an extension to Multipath TCP (MPTCP) that is meant to assess whether a path used to establish a given subflow is MPTCP-friendly, i.e., intermediate nodes involved in that path do not alter nor strip MPTCP options, which would prevent the establishment of MPTCP communications along that path. A new flag bit, called Probe Flag (P-flag) is defined for this purpose.

This document updates [RFC6824](#).

Requirements Language

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](#)].

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 <http://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 7, 2016.

Internet-Draft

MPTCP Probing

July 2015

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	The Problem	3
3.	Probe Flag (P-flag)	3
4.	Security Considerations	6
5.	IANA Considerations	6
6.	Acknowledgements	6
7.	References	6
7.1.	Normative References	6
7.2.	Informative References	6
	Authors' Addresses	6

[1.](#) Introduction

This document specifies an extension to Multipath TCP (MPTCP, [\[RFC6824\]](#)) that is meant to assess whether a path used to establish a given subflow is MPTCP-friendly. That is, intermediate nodes involved in that path do not alter nor strip MPTCP options, which would prevent the establishment of MPTCP communications along that path.

The problem is summarized briefly in [Section 2](#) while the probe flag is defined in [Section 3](#).

The solution proposed in this document allows to anticipate failures due to the presence of MPTCP-unfriendly devices in the communication paths.

[2.](#) The Problem

MPTCP supports a backup mode that relies on a dedicated flag, called backup flag carried in the MP_JOIN option: when set, this flag informs the remote peer that this is a backup subflow. Several problems may be arise such as. For example:

- o A peer decides to use a backup subflow but MPTCP cannot be used for that subflow because an intermediate function removes DSS options, for example. This failure will have a negative impact on the quality of experience.
- o Several subflows can be candidate to be used as backup but the participating nodes do not know in advance whether associated forwarding paths are MPTCP-friendly, i.e., they can actually support MPTCP subflows. The participating nodes need some "hints" to decide which subflows are to be used as regular ones and those as backup. This lack of information may also affect the perceived quality of experience.

[3.](#) Probe Flag (P-flag)

As a solution to the problem described in [Section 2](#), a meaning is associated with one of the reserved bits in MP_JOIN. This new flag bit is called: Probe Flag (P-flag). This flag bit is used to explicitly inform the remote peer that a probing procedure is associated with the corresponding subflow.

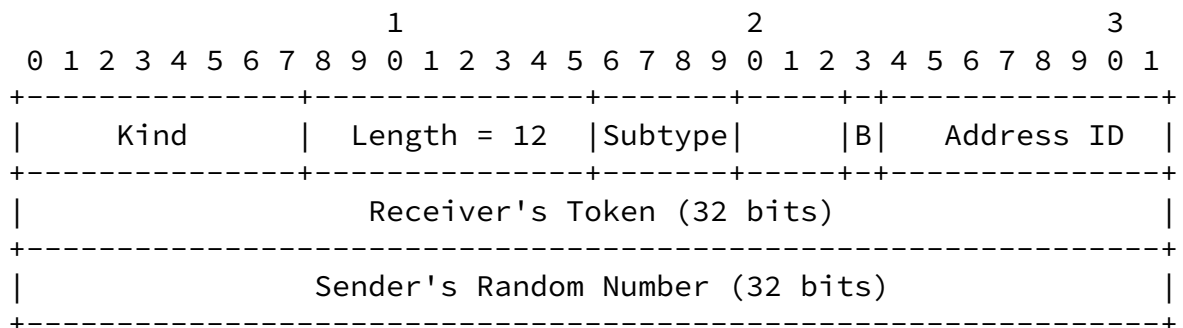
Figure 1 and Figure 2 show the required update to the MP_JOIN option format in SYN and SYN/ACK.

Internet-Draft

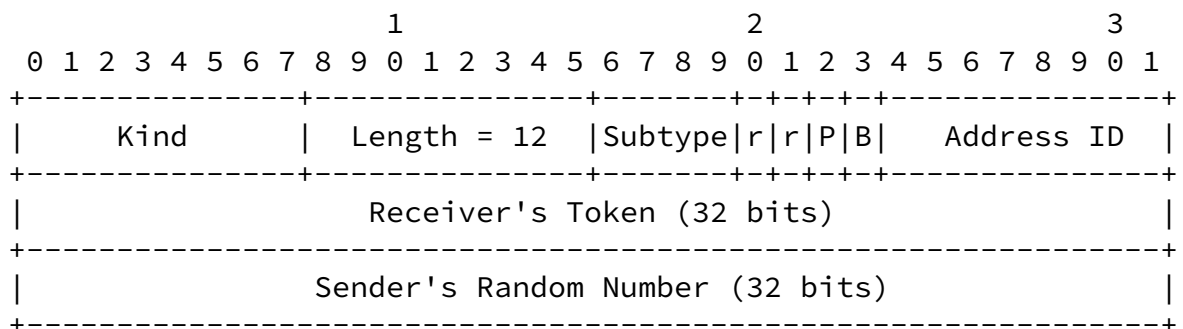
MPTCP Probing

July 2015

OLD:



NEW:



where "rr" are reserved bits for future assignment as additional flag bits. r bits MUST each be sent as zero and MUST be ignored on receipt.

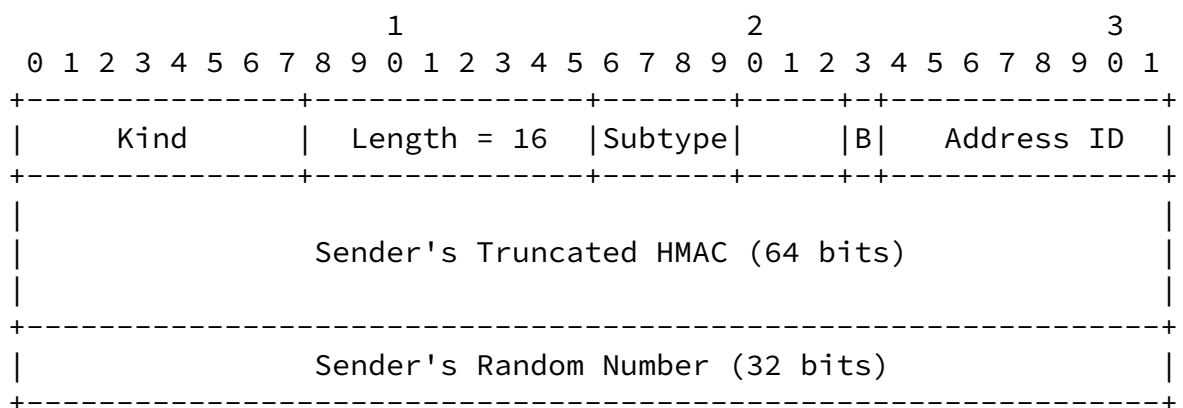
Figure 1: Join Connection (MP_JOIN) Option (for Initial SYN)

Internet-Draft

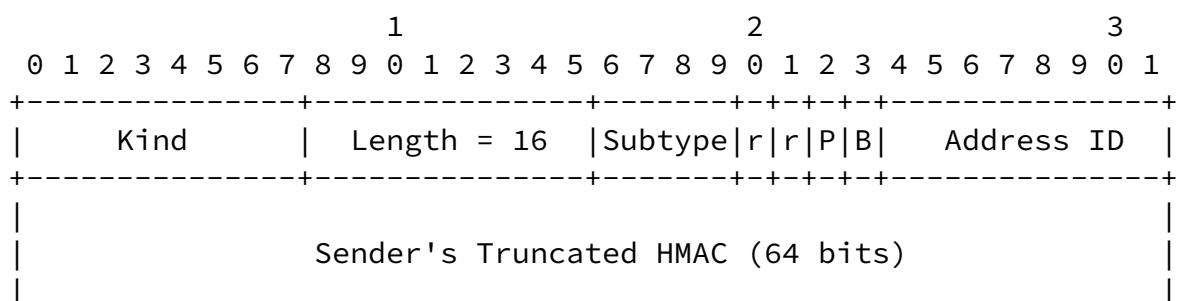
MPTCP Probing

July 2015

OLD:



NEW:



[7.](#) References

[7.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", [RFC 6824](#), January 2013.

[7.2.](#) Informative References

- [I-D.ietf-mptcp-attacks]
Bagnulo, M., Paasch, C., Gont, F., Bonaventure, O., and C. Raiciu, "Analysis of MPTCP residual threats and possible fixes", [draft-ietf-mptcp-attacks-04](#) (work in progress), March 2015.

Authors' Addresses

Mohamed Boucadair
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Christian Jacquenet
France Telecom
Rennes 35000
France

Email: christian.jacquenet@orange.com

