Network Working Group   Network Working Group
Internet-Draft   D. Borman
Intended Status: Informational   Wind River Systems
File: draft-ietf-tcpm-tcpmss-01.txt   July 13, 2009

                        TCP Options and MSS

Status of This Memo

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

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF), its areas, and its working groups. Note that
   other groups may also distribute working documents as Internet-
   Drafts.

   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."

   The list of current Internet-Drafts can be accessed at
   http://www.ietf.org/ietf/1id-abstracts.txt.

   The list of Internet-Draft Shadow Directories can be accessed at
   http://www.ietf.org/shadow.html.

   This Internet-Draft will expire on January 13, 2010.

Copyright

Abstract

   This memo discusses what value to use with the TCP MSS option.

1. INTRODUCTION

   There has been some confusion as to what value should be filled in
   the TCP MSS option when using TCP options. RFC-879 [Postel83]
   stated:

        The MSS counts only data octets in the segment, it does not
        count the TCP header or the IP header.

    which is unclear about what to do about TCP options. RFC-1122
    [Braden89] attempted to clarify this in section 4.2.2.6, but there
    still seems to be confusion.

2. TCP Options and MSS

    The MSS value to be sent in an MSS option should be equal to the
    effective MTU minus the fixed IP and TCP headers. By ignoring both
    IP and TCP options when calculating the value for the MSS option, if
    there are any IP or TCP options to be sent in a packet, then the
    sender must decrease the size of the TCP data accordingly. The
    reason for this can be seen in the following table:

	MSS is adjusted to include options	MSS isn't adjusted to include options
Sender adjusts length for options	Packets are too short	Packets are the correct length
Sender doesn't adjust length for options	Packets are the correct length	Packets are too long.

    Since the goal is to not send IP datagrams that have to be
    fragmented, and packets sent with the constraints in the lower right
    of this grid will cause IP fragmentation, the only way to guarantee
    that this doesn't happen is for the data sender to decrease the TCP
    data length by the size of the IP and TCP options. It follows then,
    that since the sender will be adjusting the TCP data length when
    sending IP and TCP options, there is no need to include the IP and
    TCP option lengths in the MSS value.

3. Security Considerations

    Packets that are too long will either be fragmented or dropped. If
    packets are fragmented, intermediary firewalls or middle boxes may
    drop the fragmented packets. In either case, when packets are

dropped the connection can fail; hence it is best to avoid generating
fragments.

4. IANA Considerations

   This document has no actions for IANA.

---

5. References

   Informative References

      [Braden89] Braden, R., editor, "Requirements for Internet Hosts --
      Communication Layers", RFC-1122, October, 1989

      [Postel83] Postel, J., "The TCP Maximum Segment Size and Related
      Topics", RFC-879, ISI, November 1983.

Authors' Addresses

   David Borman
   Wind River Systems
   Mendota Heights, MN 55120

   Phone: (651) 454-3052
   Email: david.borman@windriver.com

Full Copyright Statement