IPv6 Tunnel MTU Configuration
draft-liu-6man-tunnel-mtu-config-00

Abstract

It is not specific about how to decide IPv6 tunnel MTU in IPv6 tunneling mechanisms in some situations. This document describes the problem and provides a general solution to decide tunnel MTU 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 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 April 24, 2014.

Copyright Notice

Copyright (c) 2013 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.
1. Introduction

IPv6 tunneling mechanism defined in [RFC2473] provides support for various protocols to work in IPv6-only network. Because IPv6 intermediate routers do not support fragmentation, an IPv6 tunnel packet may be discarded by an intermediate router if the packet size exceeds the next-hop MTU. Thus, the tunnel MTU of IPv6 tunnel nodes should be well decided and managed in order to eliminate data loss.

But [RFC2473] is not specific about how to decide tunnel MTU, when a tunnel entry-point connects to multiple tunnel exit-points. It is also not clear about how to decide tunnel MTU without Path MTU Discovery [RFC1981]. This document describes the problems and proposes a solution to specify the behavior of tunnel entry-point to configure its tunnel MTU.

2. 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 [RFC2119].

3. Terminology

Terminology defined in [RFC2473] is used extensively in this document.

4. Problem Statement

Section 6.7 of [RFC2473] defines the behavior of the IPv6 tunnel entry-point to set its tunnel MTU that:

"The tunnel MTU is set dynamically to the Path MTU between the tunnel entry-point and the tunnel exit-point nodes, minus the size
of the tunnel headers"

"The tunnel entry-point node performs Path MTU discovery on the path between the tunnel entry-point and exit-point nodes"

However, it is unspecific about how a tunnel entry-point sets its tunnel MTU without performing Path MTU discovery. As IPv6 tunneling is the foundation of several IPv6 transition mechanisms, but some of these mechanisms require tunnel end-nodes not to perform Path MTU discovery. DS-Lite [RFC6333] handles this by increasing the MTU size of all the links in the path by at least 40 bytes. MAP-E [I-D.ietf-softwire-map] strongly recommends to well manage the MTU of links in the whole MAP domain, which is similar to what DS-Lite does, and specifies that "A MAP BR SHOULD NOT by default use Path MTU discovery across the MAP domain" in section 8.3.1 of [I-D.ietf-softwire-map].

In [RFC2473], tunnel MTU is defined as the Path MTU between the tunnel entry-point and the tunnel exit-point nodes minus the size of the tunnel header. In some cases, a single tunnel entry-point may connect to multiple tunnel exit-points, e.g. the IPv6 address of the tunnel exit-point is a multicast or an anycast address, or the tunnel entry-point works as an AFTR element [RFC6333].

Figure 1 shows an example that a tunnel entry-point is connecting to 2 tunnel exit-points. When the tunnel entry-point sends a tunnel packet of length 1500 to tunnel exit-point1, the packet is discarded by the intermediate router and the router sends an ICMPv6 "Packet Too Big"(PTB) message to tunnel entry-point with the MTU field equals 1280. After received the ICMPv6 PTB message, the tunnel entry-point sets its tunnel MTU to 1280-40=1240 according to section 6.7 of [RFC2473]. After that, when the tunnel entry-point sends tunnel packets to tunnel exit-point2, the tunnel packet size will be restricted to 1280. This is inefficient.

```
+-------------+  +-------+  +-------------+  +----+---+          +-------------+
| MTU=1280 | IPv6 Tunnel | | IPv4 | |  |  |  |          |                  |
| +-------+ exit-point1 +--+ host2 | +-------------+  +--------+          +-------------+
| MTU=1500 |                  |                  |                  |                  |
```

Figure 1: An Example of IPv6 Tunneling Scenario

5. Tunnel MTU Configuration
An IPv6 tunnel entry-point node SHOULD perform Path MTU discovery dynamically on the paths between the tunnel entry-point itself and each exit-point node it connects to. The PMTU information SHOULD be stored in a table indexed by the destination IPv6 address as is described in section 5.2 of [RFC1981]. When a packet enters the tunnel, the tunnel entry-point looks up the PMTU table for the corresponding PMTU value. If not found, it uses the MTU of IPv6 next-hop link as the default value. This PMTU value minus the size of the tunnel headers is set as the tunnel MTU value.

If the IPv6 tunnel entry-point node does not perform Path MTU discovery to decide its tunnel MTU, the network operator MUST estimate a safe MTU value and configure this value as the tunnel MTU. This safe MTU value should be no larger than the minimum Path MTU between the tunnel node and every potential tunnel exit-point, minus the size of tunnel headers. If the operator cannot decide this value, the tunnel MTU SHOULD be set to 1280 minus the size of tunnel headers.

6. Security Considerations

TBD

7. IANA Considerations

This document does not include an IANA request.

8. References

8.1. Normative References


8.2. Informative References

[I-D.ietf-softwire-map]
Troan, O., Dec, W., Li, X., Bao, C., Matsushima, S.,


Authors’ Addresses

Yong Cui
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing 100084
P.R.China

Phone: +86-10-6260-3059
Email: yong@csnet1.cs.tsinghua.edu.cn

Cong Liu
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing 100084
P.R.China

Phone: +86-10-6278-5822
Email: gnocuil@gmail.com