Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 24, 2014

J. Wu
C. Liu
Y. Cui
Tsinghua University

October 21, 2013

Identifying Addresses of IPv6 Tunnel Packets at Tunnel Exit-point
draft-liu-6man-ident-tunnel-packet-addr-00

Abstract

In the networks where IPv6 tunneling is used, it is not specific about how a tunnel end-node identifies the received tunnel packets by checking the destination and source addresses. when the tunnel end-node is configured with multiple IPv6 addresses or multiple IPv6 tunnel instances, such identification is necessary. This document describes the problem and defines the behavior of IPv6 tunnel end-nodes about identifying tunnel packets.

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.

Table of Contents

1. Introduction 2
2. Requirements Language 2
3. Terminology 2
4. Problem Statement 3
5. Tunnel End-node Behavior 4
5.1. Acceptable Local/Remote Address Set Maintenance 4
5.2. Inbound Tunnel Packet Identification 4
6. Security Considerations 4
7. IANA Considerations 5
8. References 5
8.1. Normative References 5
8.2. Informative References 5
Authors' Addresses 5

1. Introduction

IPv6 tunneling mechanism [RFC2473] provides support for various protocols to work in IPv6-only network. But when a tunnel end-node receives a tunnel packet, it is not specific about whether or not the tunnel end-node should identify the tunnel packet by checking the destination and source addresses in the packet. When the tunnel end-node is configured with multiple IPv6 tunnel instance, it is also undefined how to dispatch the received tunnel packet to each tunnel instance. This document provides a solution to this problem by defining the behavior of tunnel end-node on how to identify received tunnel packets.

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

This document makes use of the following terms:

Acceptable Local Address Set: A set of one or more IPv6 addresses or prefixes maintained by a tunnel instance. It represents the set of acceptable IPv6 destination addresses in the received IPv6 tunnel packets.

	Usually it consists of one or more IPv6 addresses on local interfaces of the tunnel end-node.
Acceptable Remote Address Set:	A set of one or more IPv6 addresses or prefixes maintained by a tunnel instance. It represents the set of acceptable IPv6 source addresses in the received IPv6 tunnel packets.

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

4. Problem Statement

Consider an IPv6 tunnel end-node with multiple IPv6 addresses configured on its interface. One of the IPv6 addresses is chosen as the tunnel entry-point node address [RFC2473]. When the tunnel end-node receives an IPv6 tunnel packet with its destination address other than the tunnel entry-point node address, the tunnel end-node either discards it or accepts it. Section 3.3 of [RFC2473] states that:

> "Upon receiving an IPv6 packet destined to an IPv6 address of a tunnel exit-point node, its IPv6 protocol layer processes the tunnel headers."

According to this statement, the tunnel end-node ought to accept the tunnel packet. However, when the destination IPv6 address is used to distinguish among multiple tunnel instances running in the same tunnel end-node, one tunnel packet may be passed to multiple tunnel instances, and it may not be the expected result.

When there are multiple tunnel instances in a tunnel end-node and each instance with a separated process engine, it must be decided about which tunnel instance(s) to be chosen to process a received IPv6 tunnel packet. As the payload of a IPv6 tunnel packet may be various protocols, only 3 items may be used to identify a tunnel packet: IPv6 destination address, IPv6 source address, and the payload protocol type (the Next Header field in IPv6 tunnel packet). The payload protocol type can be used to distinguish between an IPv4-in-IPv6 tunnel and an IPv6-in-IPv6 tunnel. The IPv6 source and destination address can be used to distinguish among tunnels of the same protocol type.

There are several IPv6 transition mechanisms relies on point-to-multipoint IPv6 tunnel, such as DS-Lite [RFC6333], Lightweight 4over6 [I-D.ietf-softwire-lw4over6], MAP-E [I-D.ietf-softwire-map], etc. In

these mechanisms, one tunnel instance may have multiple remote tunnel-ends, each with different IPv6 unicast addresses. Thus, the acceptable destination / source address of a inbound tunnel packet could be multiple address.

5. Tunnel End-node Behavior

5.1. Acceptable Local/Remote Address Set Maintenance

An IPv6 tunnel end-node maintains an Acceptable Local Address Set in each of its tunnel instance. An Acceptable Local Address Set contains one or more IPv6 addresses or prefixes. The destination address of an inbound IPv6 tunnel packet to be passed to a tunnel instance MUST match a record in the Acceptable Local Address Set of the tunnel instance.

An IPv6 tunnel end-node maintains an Acceptable Remote Address Set in each of its tunnel instance. An Acceptable Remote Address Set contains one or more IPv6 addresses or prefixes. The source address of an inbound IPv6 tunnel packet to be passed to a tunnel instance MUST match a record in the Acceptable Remote Address Set of the tunnel instance.

For example, in a point-to-point IPv6 tunnel, the Acceptable Local Address Set contains one IPv6 address(tunnel entry-point node address [RFC2473]), and the Acceptable Remote Address Set contains one IPv6 address(tunnel exit-point node address [RFC2473]). In the tunnel model of DS-Lite AFTR [RFC6333], the Acceptable Remote Address Set may contains a IPv6 prefix ::/0, to represent that the tunnel accepts tunnel packets from any B4s.

5.2. Inbound Tunnel Packet Identification

When an IPv6 tunnel end-node receives an IPv6 tunnel packet, the tunnel end-node identifies the packet by comparing its IPv6 source address, IPv6 destination address and protocol type (Next Header) with the Acceptable Remote Address Set, Acceptable Local Address Set, and protocol type of each tunnel instance running on the node. If all the 3 fields match, the IPv6 tunnel packet is passed to the tunnel instance.

If a tunnel packet matches more than one tunnel instance, it is passed to each of the tunnel instances. If a tunnel packet matches no tunnel instance, the tunnel end-node MUST discard the packet, and SHOULD send a ICMPv6 error message to the source address of the tunnel packet. ICMPv6 type is TBD.

6. Security Considerations

TBD

7. IANA Considerations

This document does not include an IANA request.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

8.2. Informative References

[I-D.ietf-softwire-lw4over6] Cui, Y., Qiong, Q., Boucadair, M., Tsou, T., Lee, Y., and I. Farrer, "Lightweight 4over6: An Extension to the DS-Lite Architecture", draft-ietf-softwire-lw4over6-01 (work in progress), July 2013.

[I-D.ietf-softwire-map] Troan, O., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, "Mapping of Address and Port with Encapsulation (MAP)", draft-ietf-softwire-map-08 (work in progress), August 2013.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, August 2011.

Authors' Addresses

Jianping Wu
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing 100084
P.R.China

Phone: +86-10-6278-5983
Email: jianping@cernet.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

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