JPCERT CC®

# IPv6 Security Test Manual

## (For General Release)

## 2013 Edition

**JPCERT Coordination Center**

**2014/04/28**

# 1. IPv6 Security Test 2013

## 1.1 Overview of the security test

The "IPv6 security test" is undertaken to verify the security issues of IPv6-enabled devices. This test will be conducted by vendors of applicable devices according to the test items and procedures prepared by the JPCERT Coordination Center (hereafter, JPCERT/CC), and the verification results will be published on the JPCERT/CC website as the "IPv6 Security Test Verified Products List (2013)."
This document and the "IPv6 Security Test Verified Products List (2013)" are intended for use as reference materials by the system administrators of companies and other organizations considering the purchase of IPv6-enabled devices.

See below for details on JPCERT/CC's initiative related to IPv6.

Initiative on Security Issues of the IPv6 Protocol
https://www.jpcert.or.jp/pr/2013/ipv6project.html

Vendors who agree with the aims of this initiative and wish to have their products included on the "IPv6 Security Test Verified Products List" shall conduct verification according to this IPv6 Security Test Manual, record the test results on the Information Provision Form and send it to a JPCERT/CC representative.

## 1.2 Points to note

1. Verification information provided will be published on the JPCERT/CC website, including the "IPv6 Security Test Verified Products List."
2. Models and versions to be verified shall be selected by each vendor.
3. As a rule, information provided will be listed as is. Each vendor shall check in advance to make sure no information that is not intended for publication is included.
4. Questions regarding individual verification results included on the IPv6 Security Test Verified Products List shall be directed to each vendor.

## 1.3 IPv6 Security Test 2013 verification items

Verification items for 2013 are comprised of the following 15 items. Refer to the "Investigation Report on Vulnerabilities Relating to the IPv6 Protocol Specifications" (hereafter, "investigation report") regarding vulnerabilities covered by each item.

*** The investigation report is provided only to product developers.**

| Item # | Item Name | Item Identifier |
|---|---|---|
| 1 | Disabling the processing of Type 0 Routing Headers | 2013-ipv6sec-0001 |
| 2 | DoS attacks against routers by Hop-by-Hop Options Headers | 2013-ipv6sec-0002 |
| 3 | Implementation issues in using the Jumbo Payload option | 2013-ipv6sec-0003 |
| 4 | Responding to the overwrite of packet information by illegal fragment headers: Complete overwrite (Part 1) | 2013-ipv6sec-0004 |
| 5 | Responding to the overwrite of packet information by illegal fragment headers: Complete overwrite (Part 2) | 2013-ipv6sec-0005 |
| 6 | Responding to the overwrite of packet information by illegal fragment headers: Partial overwrite (Part 1) | 2013-ipv6sec-0006 |
| 7 | Responding to the overwrite of packet information by illegal fragment headers: Partial overwrite (Part 2) | 2013-ipv6sec-0007 |
| 8 | DoS attacks using small fragment headers<br>Confirmation of tiny fragment implementation | 2013-ipv6sec-0008 |
| 9 | DoS attacks using small fragment headers<br>Large volumes of tiny fragments | 2013-ipv6sec-0009 |
| 10 | DoS attacks by sending only the first fragment packet | 2013-ipv6sec-0010 |
| 11 | DoS attacks using single fragment headers<br>Confirmation of atomic fragment implementation | 2013-ipv6sec-0011 |
| 12 | DoS attacks using single fragment headers<br>Large volumes of atomic fragments | 2013-ipv6sec-0012 |
| 13 | Attacks by off-the-route attackers via fragment ID prediction | 2013-ipv6sec-0013 |
| 14 | DoS attacks against routers using neighbor search services | 2013-ipv6sec-0014 |
| 15 | DoS attacks by sending large volumes of illegal packets to routers | 2013-ipv6sec-0015 |

## 2. Verification Procedure

### 2.1 Verification environment and implementation steps

<Deleted in the general-release version>

### 2.2 Before starting verification

<Deleted in the general-release version>

### 2.3 How to evaluate verification items susceptible to DoS

It is extremely difficult to take measures against DoS attacks. A common approach is to use a firewall or other external devices. In this verification, it was assumed that external devices would be used as a fundamental countermeasure in the event of a DoS attack, and devices were evaluated for the absence of any impact such as reboot when under attack and for the ability to return to the original state after coming under attack.

| Evaluation criteria for verification items susceptible to DoS |
|---|
| 1. Does not reboot |
| 2. Does not hang up |
| 3. Returns to a normal state after coming under a DoS attack |

## 3. Evaluation of Each Item

### (1) Disabling the processing of Type 0 Routing Headers

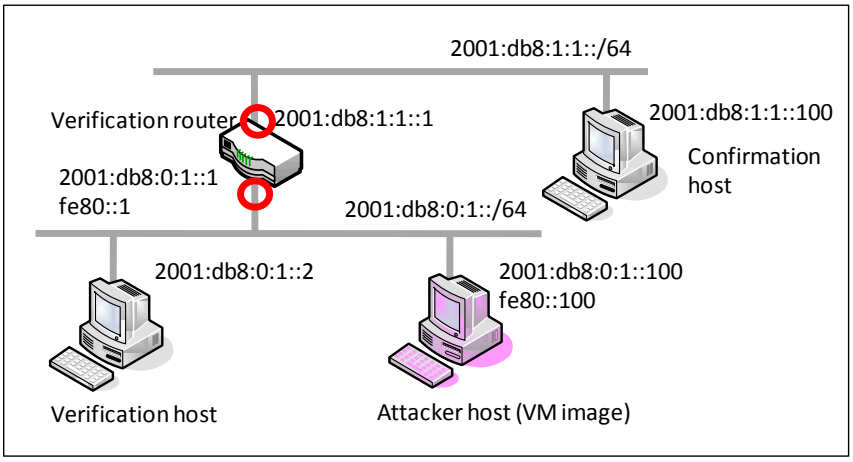
**[Identification Number]**

2013-ipv6sec-0001

**[Comparison with IPv4]**

A similar problem exists with the source routing option in IPv4

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The verification tool results indicate FAILED

## (2) **DoS attacks against routers by Hop-by-Hop Options Headers**

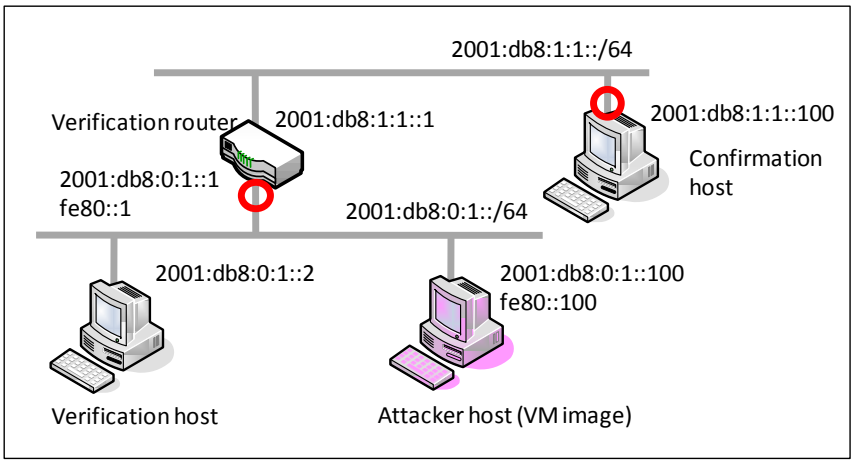
**[Identification Number]**

2013-ipv6sec-0002

**[Comparison with IPv4]**

A similar problem exists with the header option in IPv4

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The verification tool results indicate FAILED

## (3) **Implementation issues in using the Jumbo Payload option**

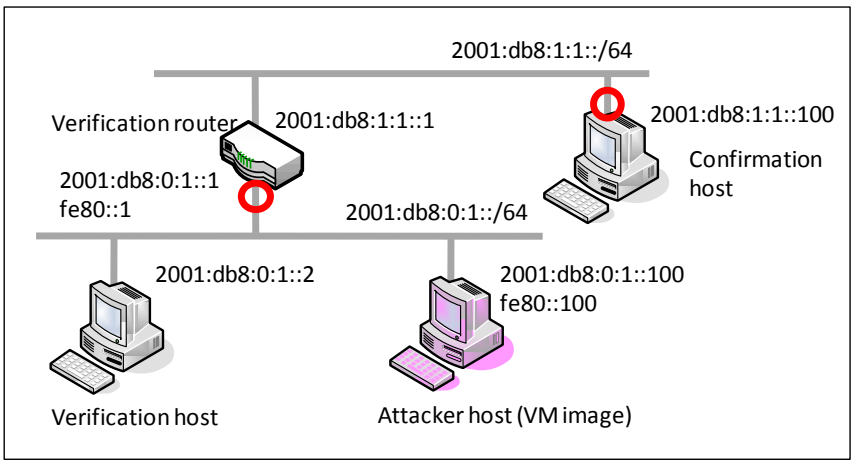
**[Identification Number]**

2013-ipv6sec-0003

**[Comparison with IPv4]**

A unique problem for IPv6

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The device under verification meets the following DoS evaluation criteria

- Does not reboot
- Does not hang up
- Returns to a normal state after coming under a DoS attack

Execute ping6 2001:db8:1:1::100 from before to after the attack, and confirm that the device returns to a normal state

## (4) Responding to the overwrite of packet information by illegal fragment headers: Complete overwrite (Part 1)

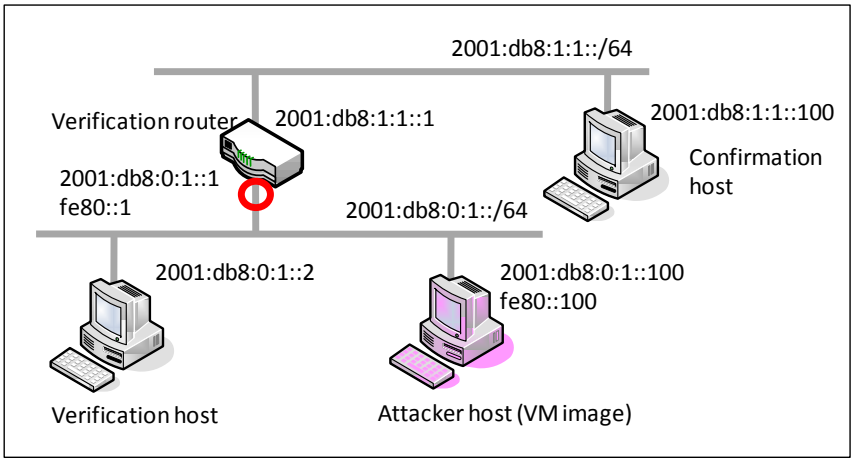
**[Identification Number]**

2013-ipv6sec-0004

**[Comparison with IPv4]**

A similar problem exists with IPv4 fragments

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The verification tool results indicate FAILED

## (5) Responding to the overwrite of packet information by illegal fragment headers: Complete overwrite (Part 2)

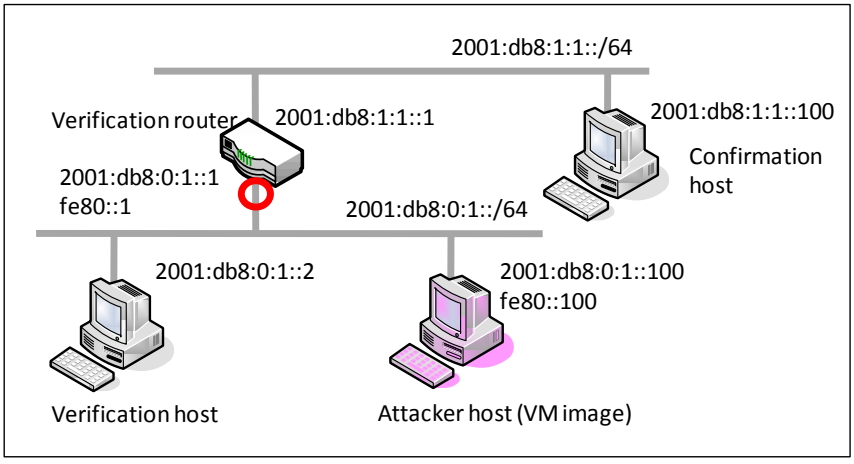
**[Identification Number]**

2013-ipv6sec-0005

**[Comparison with IPv4]**

A similar problem exists with IPv4 fragments

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The verification tool results indicate FAILED

## (6) Responding to the overwrite of packet information by illegal fragment headers: Partial overwrite (Part 1)

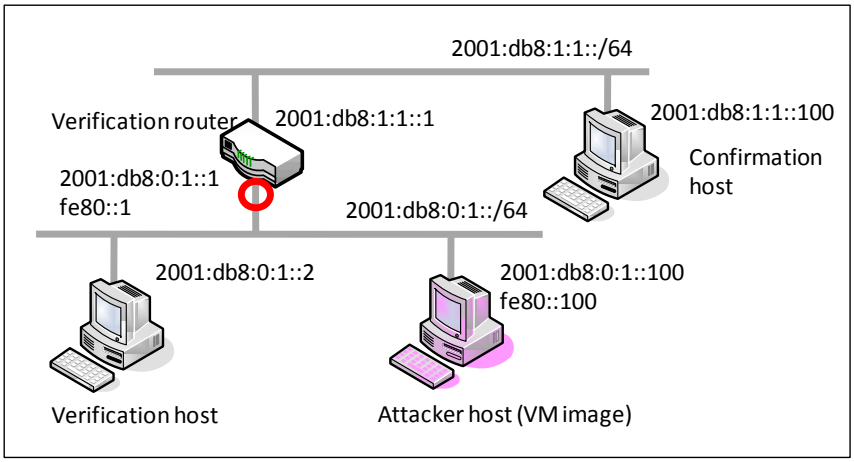
**[Identification Number]**

2013-ipv6sec-0006

**[Comparison with IPv4]**

A similar problem exists with IPv4 fragments

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The verification tool results indicate FAILED

## (7) Responding to the overwrite of packet information by illegal fragment headers: Partial overwrite (Part 2)

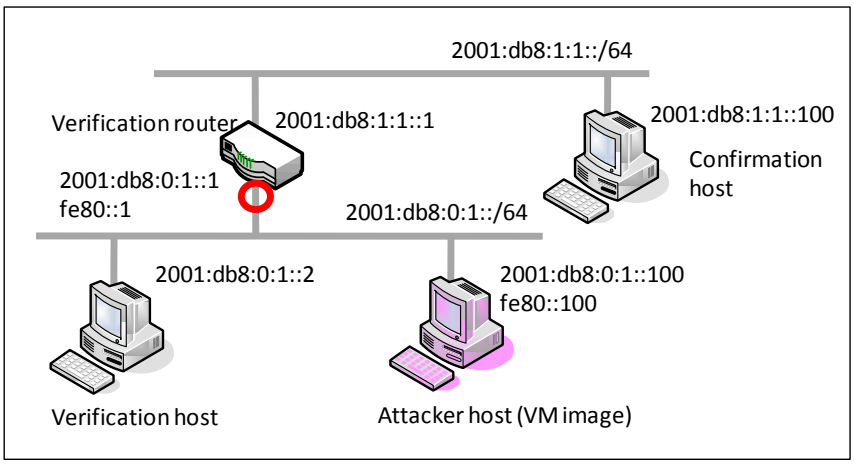
**[Identification Number]**

2013-ipv6sec-0007

**[Comparison with IPv4]**

A similar problem exists with IPv4 fragments

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The verification tool results indicate FAILED

## (8) DoS attacks using small fragment headers—Confirmation of tiny fragment implementation

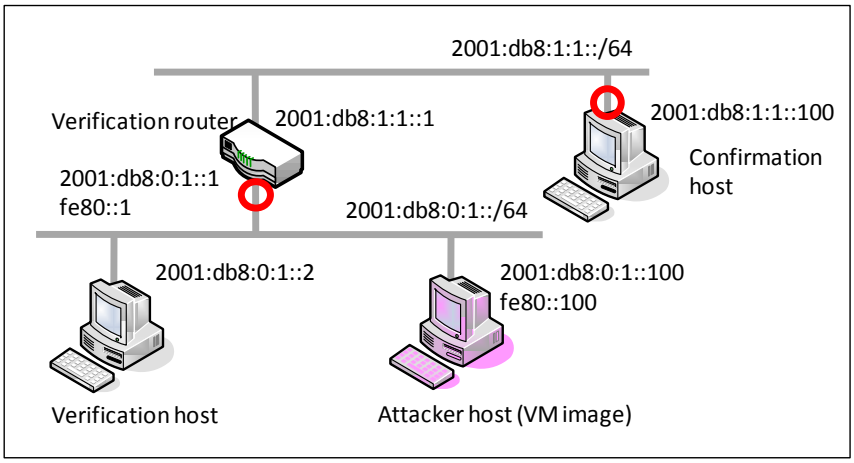
**[Identification Number]**

2013-ipv6sec-0008

**[Comparison with IPv4]**

A similar problem exists with IPv4 fragments

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The device under verification meets the following DoS evaluation criteria

- Does not reboot
- Does not hang up
- Returns to a normal state after coming under a DoS attack

Execute ping6 2001:db8:1:1::100 from before to after the attack, and confirm that the device returns to a normal state

## (9) **DoS attacks using small fragment headers—Large volumes of tiny fragments**

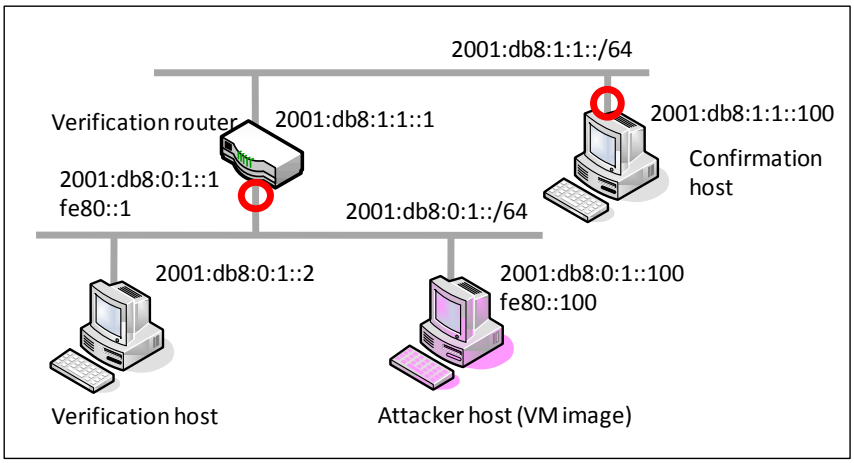
**[Identification Number]**

2013-ipv6sec-0009

**[Comparison with IPv4]**

A similar issue exists with IPv4 fragments

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The device under verification meets the following DoS evaluation criteria

- Does not reboot
- Does not hang up
- Returns to a normal state after coming under a DoS attack

Execute ping6 2001:db8:1:1::100 from before to after the attack, and confirm that the device returns to a normal state

## (10) **DoS attacks by sending only the first fragment packet**

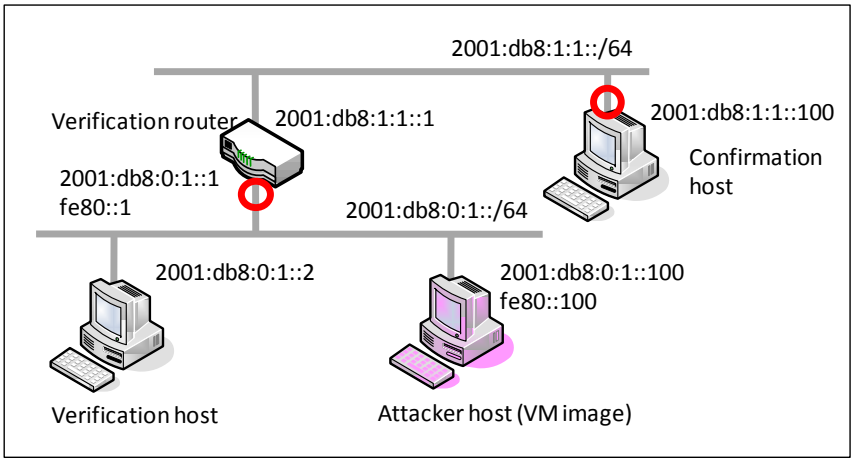
**[Identification Number]**

2013-ipv6sec-0010

**[Comparison with IPv4]**

A similar issue exists with IPv4 fragments

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The device under verification meets the following DoS evaluation criteria

- Does not reboot
- Does not hang up
- Returns to a normal state after coming under a DoS attack

Execute ping6 2001:db8:1:1::100 from before to after the attack, and confirm that the device returns to a normal state

## (11) DoS attacks using small fragment headers—Confirmation of atomic fragment implementation

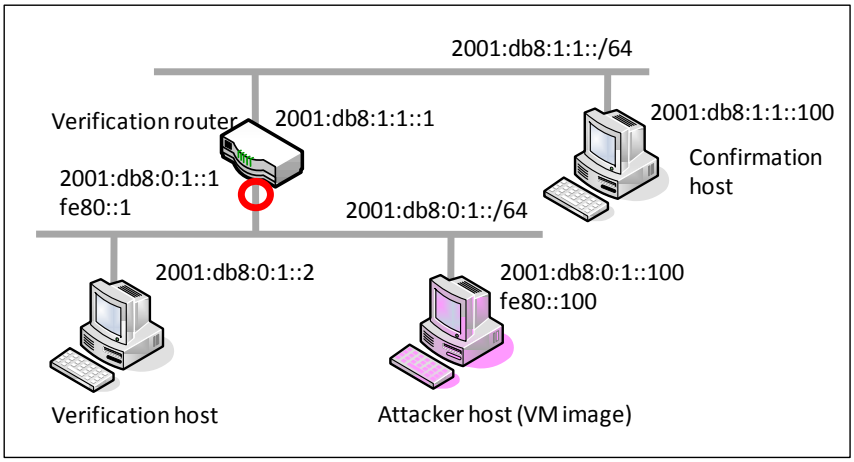
**[Identification Number]**

2013-ipv6sec-0011

**[Comparison with IPv4]**

A unique issue for IPv6

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The verification tool results indicate PASSED

## (12) **DoS attacks using single fragment headers—Large volumes of atomic fragments**

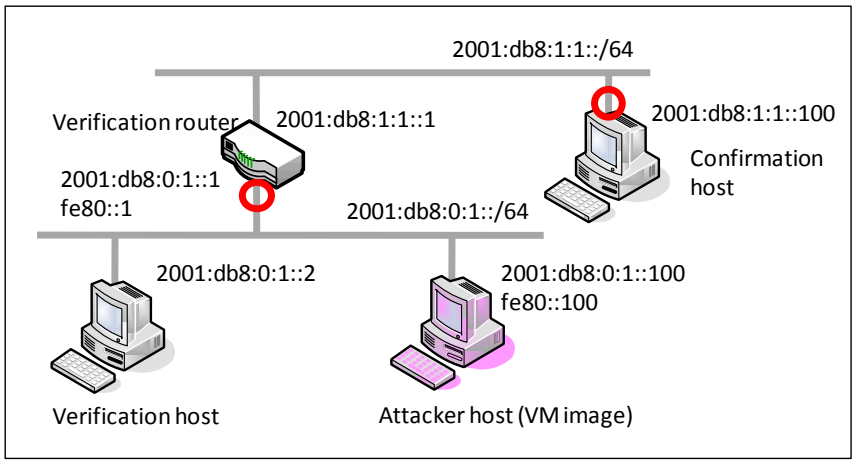
**[Identification Number]**

2013-ipv6sec-0012

**[Comparison with IPv4]**

A unique issue for IPv6

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The device under verification meets the following DoS evaluation criteria

- Does not reboot
- Does not hang up
- Returns to a normal state after coming under a DoS attack

Execute ping6 2001:db8:1:1::100 from before to after the attack, and confirm that the device returns to a normal state

## (13) **Attacks by off-the-route attackers via fragment ID prediction**

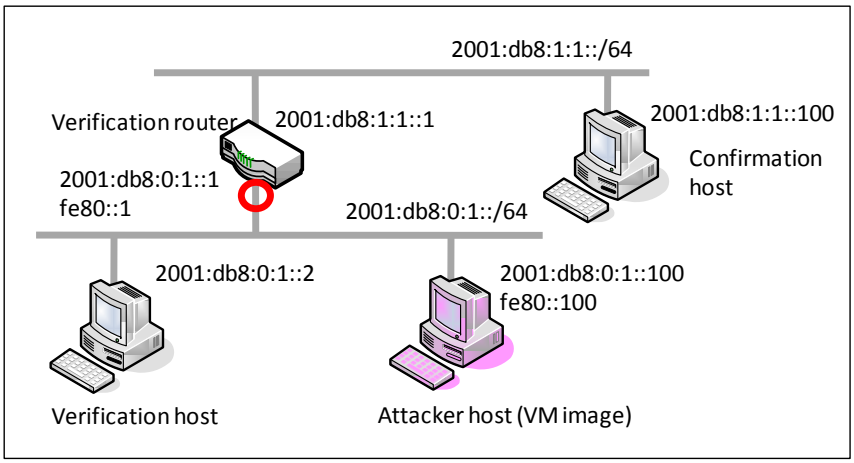
**[Identification Number]**

2013-ipv6sec-0013

**[Comparison with IPv4]**

A similar problem exists with IPv4 fragments

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The verification tool results indicate "Randomized IDs"

## (14) **DoS attacks against routers using neighbor search services**

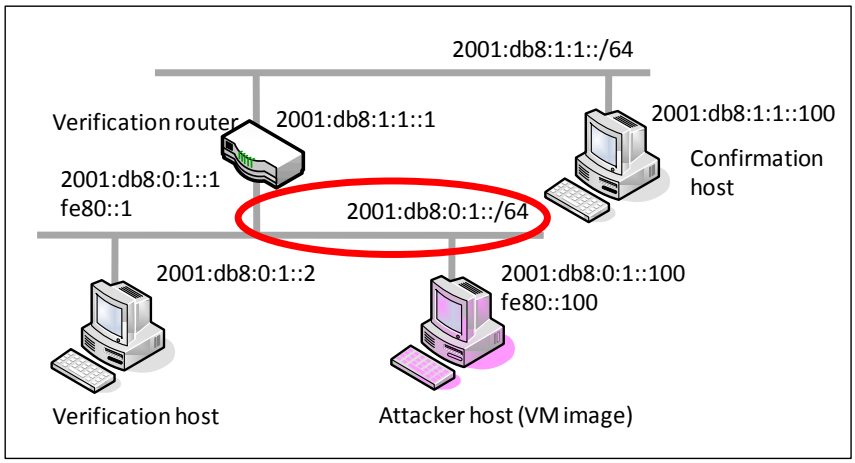
**[Identification Number]**

2013-ipv6sec-0014

**[Comparison with IPv4]**

A similar problem exists with the ARP in IPv4

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The device under verification meets the following DoS evaluation criteria

- Does not reboot
- Does not hang up
- Returns to a normal state after coming under a DoS attack

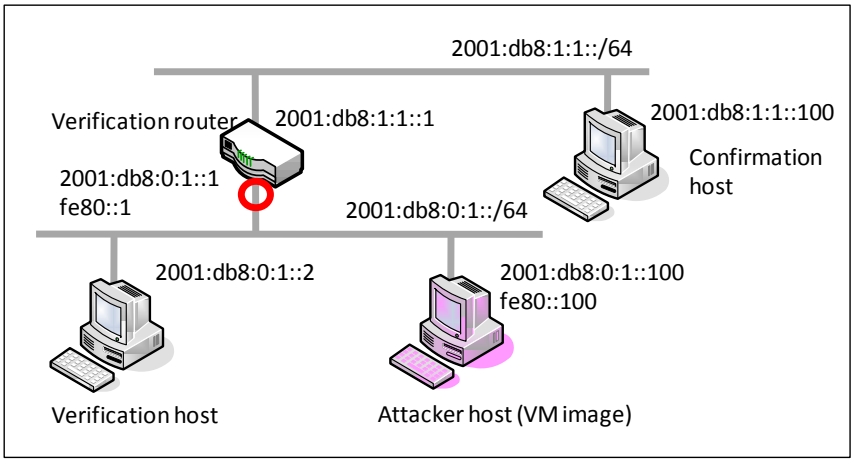
Execute ping6 2001:db8:1:1::100 from before to after the attack, and confirm that the device returns to a normal state

## (15) DoS attacks by sending large volumes of illegal packets to routers—(Echo requests divided into a size smaller than the size of MTU)

**[Identification Number]**

2013-ipv6sec-0015

**[Verification Configuration]**




**[Verification Procedure]**

<Deleted in the general-release version>

**[Example of Verification Results]**

<Deleted in the general-release version>

**[Determination of Pass/Failure]**

The device under verification meets the following DoS evaluation criteria

- Does not reboot
- Does not hang up
- Returns to a normal state after coming under a DoS attack

Execute ping6 2001:db8:1:1::100 from before to after the attack, and confirm that the device returns to a normal state.