

6Man
Internet-Draft
Expires: April 19, 2012

J. Halpern
Ericsson
October 17, 2011

Mitigating Neighbor Discovery Based Denial of Service Attacks
draft-halpern-6man-nddos-mitigation-00

Abstract

It has been observed that with the large space of IPv6 addresses within a subnet, remote attackers can send packets that saturate a routers ND cache, and potentially saturate a subnet with ND Solicitation messages as well. Some operational techniques and small protocol adjustments have been proposed that can help alleviate this problem. This draft proposes a slightly more drastic optional behavior for routers, which can nearly eliminate this problem.

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 19, 2012.

Copyright Notice

Copyright (c) 2011 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 [3](#)
[2.](#) Terminology [3](#)
[3.](#) Problem Summary and Solution Approach [3](#)
[4.](#) Basic Behavior [4](#)
[5.](#) Protocol Enhancements [4](#)
[6.](#) IANA Considerations [5](#)
[7.](#) Security Considerations [5](#)
[8.](#) References [5](#)
 [8.1.](#) Normative References [5](#)
 [8.2.](#) Informative References [6](#)
Author's Address [6](#)

1. Introduction

It has been observed that with the large space of IPv6 addresses within a subnet, remote attackers can send packets that saturate a routers ND cache, and potentially saturate a subnet with ND Solicitation messages as well. A thorough description of the problem can be found in [[ndproblem](#)]. Some operational techniques and small protocol adjustments have been proposed that can help alleviate this problem are described in [[ndenhance](#)]. This draft proposes a slightly more drastic optional behavior for routers, which can nearly eliminate this problem.

While the basic behavior described here can be looked upon as a local matter, there are robustness issues if a router applies this solution on its own. Therefore, additional enhancements to the basic ND protocol behavior as defined in [[RFC4861](#)] are specified in this document.

2. Terminology

The terminology here follows that defined in [[RFC4861](#)]

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, HOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [[RFC2119](#)].

3. Problem Summary and Solution Approach

The basic problem under discussion is the ability for a remote attacker to fill a routers neighbor cache with unresolved, and unresolvable, entries. If done at a sufficient rate, this may prevent the router from maintaining the necessary entries for actually reaching the hosts on a subnet the router directly serves. Depending upon circumstances, the rate of Neighbor Solicitations

messages on the subnet may be high enough to cause difficulties, since these are multicast messages.

An attacker causes this problem by sending IPv6 datagrams addressed to distinct hypothetical nonexistent host systems on the subnet. The attacker sends these messages continuously. The router receives these messages, and as specified in [\[RFC4861\]](#) it generates Neighbor solicitation messages for each unknown destination, and creates INCOMPLETE Neighbor cache entries for each one. The attacker can use random destination addresses, or even sequential addresses and count on passing the actual hosts quickly. With IPv4, this problem could be coped with in most cases by simply having a table large enough for

all the values in the subnet. With IPv6, which recommends subnets be /64s, such sizing is no longer possible.

This proposal asks the question, what if the router never accepts packets for unknown hosts on local subnets? In such a case, it would never create INCOMPLETE cache entries, and would never generate Neighbor Solicitation messages based upon received traffic. Instead of soliciting such information, the router would learn of the hosts (and neighboring routers) on the subnet from received information.

[4.](#) Basic Behavior

The basic operational model for the router is still that it maintains a neighbor cache with IPv6->Media address resolution information. It populates this cache upon receiving Router Solicitation or Neighbor Advertisement messages from hosts on the subnet.

It is still important that the router be able to tell whether hosts are still reachable. As such, routers should assign lifetime information to this information. As the lifetime approaches, rather than discarding the information, the router can issue a Neighbor Solicitation message to revalidate the information. In the absence of a response, such revalidation should be attempted several times. On links where power consumption is a significant issue, it may make sense to simply keep the neighbor cache information without expiration or revalidation.

5. Protocol Enhancements

While the above description prevents the attack of concern, it has several failure modes. In particular, if a router comes up after a subnet is operational, it will not learn the necessary information. Also, it would seem desirable to provide additional robustness in the learning process, in case too many messages get lost.

There are three protocol enhancements that can be used to help this problem. The first mechanism, which has also been proposed for other reasons, is simply for all hosts on the subnet to keep sending Router Solicitation messages, rather than ceasing after only three transmissions. The rate of sending could be reduced. The message load on the subnet would not be excessive. One might want to adjust the router response to such messages, allowing the router to simply maintain the steady rate of advertisement. This would ensure the router learned of all the hosts on the network in a reasonable time even if there were unexpected behaviors (partition repair at the link level, for example) which would otherwise interfere.

As a variation on the above, one could define a "please respond" flag in the Router Advertisement, which the routers could set to intermittently to refresh information. As the repeated Router Solicitations address other issues as well, that seems preferred.

While the above enhancement would be sufficient to ensure robustness, it is desirable to be able to deploy this solution before all the hosts on the subnet are upgraded to exhibit that behavior. As such, other robustness techniques are recommended. These approaches rely on the fact that the primary problem occurs when a new router joins an active subnet with an already active serving router providing the same prefix the new router would provide.

One thing the existing router could do, which would provide the needed robustness, is to cause all the hosts it knows about to send new Neighbor Advertisements. It can do this by sending each host a Neighbor solicitation with a source address of the unspecified address. This will cause the host to multicast the Neighbor Advertisement it responds with.

One may consider that the message exchanges of such a triggering and responding sequence is excessive. As a fall-back, one could easily

define an exchange protocol by which an operational router on the subnet could send its neighbor cache to the new router. As this is more complex, more detailed work on that is deferred until it is deemed necessary.

[6.](#) IANA Considerations

There are currently no IANA considerations or assignments in this document.

[7.](#) Security Considerations

There are presumably security implications of this behavioral change, but they have not been evaluated yet.

[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.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman,

Halpern Expires April 19, 2012 [Page 5]

Internet-Draft Mitigating ND Based DoS Attacks October 2011

"Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.

[8.2.](#) Informative References

[ndproblem]
Kumari, W., Gashinsky, I., and J. Jaeggli,
"I-D.gashinsky-v6ops-v6nd-problems-00.txt", 2011.

[ندنهانه]
Kumari, W., Gashinsky, I., and J. Jaeggli,
"I-D.gashinsky-v6nd-enhance-00.txt", October 2011.

Author's Address

Joel M. Halpern
Ericsson
P. O. Box 6049
Leesburg, VA 20178
US

Email: joel.halpern@ericsson.com