6man Working Group   S. Krishnan
Internet-Draft   Ericsson
Intended status: Standards Track   D. Anipko
Expires: January 10, 2013   D. Thaler
                                                           Microsoft
                                                        July 9, 2012

               Packet loss resiliency for Router Solicitations
                     draft-krishnan-6man-resilient-rs-00

Abstract

   When an interface on a host is initialized, the host transmits Router
   Solicitations in order to minimize the amount of time it needs to
   wait until the next unsolicited multicast Router Advertisement is
   received. In certain scenarios, these router solicitations
   transmitted by the host might be lost. This document specifies a
   mechanism for hosts to cope with the loss of the initial Router
   Solicitations.

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 January 10, 2013.

Copyright Notice

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

As specified in [RFC4861], when an interface on a host is initialized, in order to obtain Router Advertisements quickly, a host transmits up to MAX_RTR_SOLICITATIONS (3) Router Solicitation messages, each separated by at least RTR_SOLICITATION_INTERVAL (4) seconds. In certain scenarios, these router solicitations transmitted by the host might be lost.

The generic scenario is that the interface on the host comes up before it gets access to a router. Examples are

a. Host is connected to a bridged residential gateway (over Ethernet or WiFi). LAN connectivity is achieved at interface initialization, but the upstream WAN connectivity is not active yet. In this case, the host just gives up after the initial RS retransmits.

b. Accesses that turn off periodic RAs and operate only in a RS triggered environment. In this case if the link between the AP and the host comes up before the link between the AP and the Controller/Router, the host will never be able to connect.

Once the initial RSs are lost, the host gives up and assumes that there are no routers on the link as specified in Section 6.3.7 of [RFC4861]. The host will not have any form of Internet connectivity until the next unsolicited multicast Router Advertisement is received. These Router Advertisements are transmitted at most MaxRtrAdvInterval seconds apart (maximum value 1800 seconds). In the worst case scenario, a host would be without any connectivity, on average, for half this period (900 seconds). This delay may be unacceptable in some scenarios.

1.1. Conventions used in this document

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].

[2](#). Proposed algorithm

   To achieve resiliency to packet loss, the host needs to continue
   retransmitting the Router Solicitations until it receives a Router
   Advertisement, or until it is willing to accept that no router
   exists. If the host continues retransmitting the RSs at
   RTR_SOLICITATION_INTERVAL second intervals, it would cause excessive
   network traffic. To achieve resiliency while keeping the network
   traffic low, the host must use some form of exponential backoff
   algorithm to retransmit the RSs.

[3](#). IANA Considerations

   This document does not require any IANA actions.

[4](#). Security Considerations

   This document does not present any additional security issues beyond
   those specified in [[RFC4861](#)].

[5](#). Acknowledgements

   The author would like to thank Steve Baillargeon for his reviews and
   suggestions that made this document better.

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

Authors' Addresses

    Suresh Krishnan
    Ericsson
    8400 Decarie Blvd.
    Town of Mount Royal, QC
    Canada

    Phone: +1 514 345 7900 x42871
    Email: suresh.krishnan@ericsson.com

    Dmitry Anipko
    Microsoft
    One Microsoft Way
    Redmond, WA
    USA

    Phone: +1 425 703 7070
    Email: danipko@microsoft.com

    Dave Thaler
    Microsoft
    One Microsoft Way
    Redmond, WA
    USA

    Email: dthaler@microsoft.com