

6man Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 27, 2011

S. Krishnan
Ericsson
O. Bonness
Deutsche Telekom AG
August 26, 2010

IPv6 Stateless auto-configuration issues due to loss of IPv6 Router
Solicitation messages
draft-krishnan-6man-rs-lost-00

Abstract

The IPv6 stateless auto-configuration(SLAAC) mechanism allows a host to generate its own addresses using a combination of locally available information and information advertised by routers. This document describes a failure scenario for SLAAC and discusses how hosts can recover from this failure in a properly configured network.

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 February 27, 2011.

Copyright Notice

Copyright (c) 2010 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

Internet-Draft

SLAAC Clarifications

August 2010

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Conventions used in this document	3
3.	Issues due to lost RSs	3
4.	Recovering from lost RSs	3
5.	Open Issues	4
6.	Acknowledgements	5
7.	Security Considerations	5
8.	IANA Considerations	5
9.	Normative References	5
	Authors' Addresses	5

1. Introduction

When an interface on an IPv6 host is initialized, To obtain Router Advertisements quickly, a host transmits Router Solicitation messages in order to elicit a Router advertisement from a router. This document analyzes the case where all of these RSs are not received by the router due to lack of connectivity at the time the RSs were transmitted.

2. 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](#)].

3. Issues due to lost RSs

When an interface on an IPv6 host is initialized, in order to obtain Router Advertisements quickly, a host SHOULD transmit up to 3 (MAX_RTR_SOLICITATIONS) Router Solicitation messages, each separated by at least 4 (RTR_SOLICITATION_INTERVAL) seconds as specified in [Section 6.3.7. of \[RFC4861\]](#).

If there exists a switched network between the host and the router on the network, it is possible that the host interface may become enabled before link layer connectivity to the router is complete. In this case the Router Solicitations sent by the host will never reach the router and hence will not elicit a Router Advertisement from the router.

After sending MAX_RTR_SOLICITATIONS solicitations, and receiving no Router Advertisements after having waited MAX_RTR_SOLICITATION_DELAY seconds after sending the last solicitation, the host will conclude that there are no routers on the link for stateless auto-

configuration purposes. Hence the host will not be able to obtain a global unicast address.

4. Recovering from lost RSs

After the RSs are lost, the host assumes that no routers are present on the link, and will no longer actively try to acquire a Router. So even if a router appears on the link due to link layer connectivity being established, the host will be blissfully oblivious to the presence of the router.

Even though the host is not actively soliciting routers at this point, it will continue to receive and process Router Advertisements messages as specified in [Section 6.3.7. of \[RFC4861\]](#).

As long as the router on the link keeps sending periodic unsolicited multicast RAs (as required by [\[RFC4861\]](#), one of these RAs will eventually reach the host. If these unsolicited RAs contain at least one prefix information option (PIO) with the autonomous address-configuration flag set, the host can start using this prefix for SLAAC [\[RFC4862\]](#) and it will successfully form an address. Hence the issue is resolved.

If the RA does not contain any PIOs or it does not contain any PIOs with the autonomous address-configuration flag set, it is unclear how the host will react. This scenario, where the unsolicited RAs contain less information than the solicited RAs, seems to be anticipated and allowed by [\[RFC4861\]](#) where the following text is present.

"Moreover, a host SHOULD send at least one solicitation in the case where an advertisement is received prior to having sent a solicitation. Responses to solicited advertisements may contain more information than unsolicited advertisements."

Hosts following the SHOULD recommendation will send an RS in response to the received unsolicited RA. This RS will cause the router to send a solicited RA that will contain a PIO with the autonomous address-configuration flag set. The host can start using this prefix for SLAAC and it will successfully form an address. Hence the issue

is resolved.

[5.](#) Open Issues

If the router does not sent periodic multicast unsolicited RAs or if the host does not implement the SHOULD recommendation for sending an RS on receipt of an unsolicited RA, the host cannot configure an address using SLAAC. In the absence of other address configuration mechanisms (DHCPv6, Manual), the host will not be able to obtain a global unicast address.

While such router behavior is clearly non-compliant and is unlikely to be encountered, the expected behavior of hosts under this situation is unclear. This document has been written in order to foster discussion about both existing and expected host behaviors in this case.

[6.](#) Acknowledgements

The authors would like to thank Alan Kavanagh, Balazs Varga, Sven Ooghe, Thomas Haag, Thomas Narten, Ole Troan and Wojciech Dec for the discussions that led to this document.

[7.](#) Security Considerations

This document describes a failure scenario for IPv6 Stateless address auto-configuration. It does not bring up any new security issues.

[8.](#) IANA Considerations

This document does not require any IANA action.

[9.](#) 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.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [RFC 4862](#), September 2007.

Authors' Addresses

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

Email: suresh.krishnan@ericsson.com

Krishnan & Bonness

Expires February 27, 2011

[Page 5]

Internet-Draft

SLAAC Clarifications

August 2010

Olaf Bonness
Deutsche Telekom AG
T-Labs (Research & Development)
Goslarer Ufer 35
10589 Berlin
Germany

Email: olaf.bonness@telekom.de

