

v6ops Working Group
Internet-Draft
Expires: January 2, 2009

G. Van de Velde
E. Levy-Abegnoli
C. Popoviciu
Cisco Systems
J. Mohacsi
NIIF/Hungarnet
July 1, 2008

IPv6 RA-Guard
<[draft-ietf-v6ops-ra-guard-00.txt](#)>

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on January 2, 2009.

Abstract

When using IPv6 within a single L2 network segment it is necessary to ensure that all routers advertising their services within it are valid. In cases where it is not convenient or possible to use SeND [[RFC3971](#)] a rogue Router Advertisement (RA) [[RFC4861](#)] could be sent by accident due to misconfiguration or ill intended. Simple solutions for protecting against rogue RAs are beneficial in complementing SeND in securing the L2 domain for certain types of devices or in certain transitional situations.

Internet-Draft

IPv6 RA-Guard

July 2008

This document proposes a solution to reduce the threat of rogue RAs by enabling layer 2 devices to forward only RAs received over designated ports.

Table of Contents

1.	Introduction	3
2.	RA-guard as a deployment complement to SEND	3
3.	RA-Guard state-machine	4
3.1.	RA-Guard state: OFF	4
3.2.	RA-Guard state: LEARNING	4
3.3.	RA-Guard state: ACTIVE	5
4.	RA-Guard interface states	5
4.1.	RA-Blocking interface	5
4.2.	RA-Forwarding interface	5
4.3.	RA-Learning interface	5
4.4.	RA-Guard interface state transition	5
5.	RA-Guard Use Considerations	6
6.	IANA Considerations	6
7.	Security Considerations	6
8.	Acknowledgements	6
9.	Normative References	6
	Authors' Addresses	7
	Intellectual Property and Copyright Statements	9

1. Introduction

When operating IPv6 in a shared L2 network segment without complete SeND support by all devices connected or without the availability of the infrastructure necessary to support SeND, there is always the risk of facing operational problems due to rogue Router Advertisements generated maliciously or unintentionally by unauthorized or improperly configured routers connecting to the segment.

There are several examples of work done on this topic which resulted in several related studies [[reference1](#)] [[reference2](#)] [[reference3](#)]. This document describes a solution framework to the rogue-RA problem where network segments are designed around a single or a set of L2-switching devices capable of identifying invalid RAs and blocking them. The solutions developed within this framework can span the spectrum from basic (where the port of the L2 device is statically instructed to forward or not to forward RAs received from the connected device) to advanced (where a criteria is used by the L2 device to dynamically validate or invalidate a received RA, this criteria can even be based on SeND mechanisms).

2. RA-guard as a deployment complement to SEND

RA-guard does not intend to provide a substitute for SeND based solutions. It actually intends to provide complementary solutions in those environments where SeND might not be suitable or fully supported by all devices involved. It may take time until SeND is ubiquitous in IPv6 networks and some of its large scale deployment aspects are sorted out such as provisioning hosts with trust anchors. It is also reasonable to expect that some devices might not consider implementing SeND at all such as IPv6 enabled sensors. The RA-guard "SeND-validating" RA on behalf of hosts would potentially simplify some of these challenges.

RA-guard can be seen as a superset of SEND with regard to router authorization. Its purpose is to filter Router Advertisements based on a set of criterias, from a simplistic "RA dis-allowed on a given interface" to "RA allowed from pre-defined sources" and up to full SEND fledge "RA allowed from authorized sources only".

In addition to this granularity on the criteria for filtering out Router Advertisements, RA-guard introduces the concept of router authorization proxy. Instead of each node on the link analysing RAs and making an individual decision, a legitimate node-in-the-middle performs the analysis on behalf of all other nodes on the link. The analysis itself is not different from what each node would do: if

SeND is enabled, the RA is checked against X.509 certificates. If any other criteria is in use, such as known L3 (addresses) or L2 (link-layer address, port number) legitimate sources of RAs, the node-in-the middle can use this criteria and filter out any RA that does not comply. If this node-in-the-middle is a L2 device, it will not change the content of the validated RA, and avoid any of the nd-proxy pitfalls.

RA-guard intends to provide simple solutions to the rogue-RA problem in contexts where simplicity is required while leveraging SeND in context with a mix of SeND capable devices (L2 switches and routers) and devices that do not consistently use SeND. Futhermore, RA-guard is useful to simplify SeND deployments, as only the L2 switch and the routers are required to carry certificates -their own and the trust anchor certificates-.

3. RA-Guard state-machine

RA-Guard runs on devices that provide connectivity between hosts and other hosts or networking devices. An example of such RA-Guard capable device would be an OSI Layer-2 switch. The capability can be enabled globally at device level or at interface level.

When RA-Guard is SEND-based, the timing of the learning phase, as well as the overall behavior of the device doing RA-guard is as-defined in [[RFC3971](#)].

When RA-guard is using more static criterias, the state-machine of

the RA-Guard capability consists of three different states:

State 1: OFF

State 2: LEARNING

State 3: ACTIVE

The transition between these states can be triggered by manual configuration or by meeting a pre-defined criteria.

[3.1.](#) RA-Guard state: OFF

A device or interface in RA-Guard "OFF" state, operates as if the RA-Guard capability is not available.

[3.2.](#) RA-Guard state: LEARNING

A device or interface in the RA-Guard "Learning" state is actively acquiring information about the devices connected to its interfaces. The learning process takes place over a pre-defined period of time by capturing router advertisements or it can be event triggered. The

information gathered is compared against pre-defined criteria which qualify the validity of the RAs.

In this state, the RA-Guard enabled device or interface is either blocking all RAs until their validity is verified or, alternatively it can temporarily forward the RAs until the decision is being made.

[3.3.](#) RA-Guard state: ACTIVE

A device or interface running RA-Guard and in Active state will block ingress RA-messages deemed invalid and will forward those deemed valid based on a pre-defined criteria defined.

[4.](#) RA-Guard interface states

The interfaces of devices with the RA-guard capability enabled can be in three possible states related to RA handling: Learning, Blocking and Forwarding.

[4.1.](#) RA-Blocking interface

An interface in the RA Blocking state blocks all ingress RA messages when RA-Guard capability is activated on a device.

[4.2.](#) RA-Forwarding interface

An interface in the RA Forwarding state forwards all ingress RA messages deemed valid when RA-Guard capability is activated on a device.

[4.3.](#) RA-Learning interface

An interface in a RA Learning state snoops all received RAs and compares them against the criteria identifying valid RAs. While in this state, the RAs can be blocked or forwarded until a decision is taken regarding their validity.

[4.4.](#) RA-Guard interface state transition

In the simplest cases, an RA-Guard enabled interface can be manually set in an RA-Blocking or RA-Forwarding state. By default, the interfaces of a legitimate node-in-the-middle could be set in RA-Blocking mode and enabled for forwarding by the network administrator. In the more general case, the interface acquires RA information during the RA Learning state and by using a pre-defined validity criteria (see [section 2](#)) decides whether the analyzed RAs should be forwarded or blocked. Based on this decision, the

interface transitions into the RA Blocking or the RA Forwarding state.

Upon detecting new RAs, a port can transition back into an RA-Guard Learning state.

[5.](#) RA-Guard Use Considerations

The RA-Guard mechanism is effective only when all messages between IPv6 devices in the target environment traverse the controlled L2 networking devices. When on a shared media such as an Ethernet hub, devices can communicate directly without going through an RA-Guard capable L2 networking device. In this scenario, the RA-Guard feature cannot protect against rogue-RAs.

RA-Guard mechanism does not protect against tunneled IPv6 traffic.

6. IANA Considerations

There are no extra IANA consideration for this document.

7. Security Considerations

There are no extra Security consideration for this document.

8. Acknowledgements

The authors dedicate this document to the memory of Jun-ichiro Hagino (itojun) for his contributions to the development and deployment of IPv6.

9. Normative References

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.

[reference1]
LORIA/INRIA, "NDPMon - IPv6 Neighbor Discovery Protocol Monitor (<http://ndpmon.sourceforge.net/>)", November 2007.

Van de Velde, et al. Expires January 2, 2009 [Page 6]

Internet-Draft IPv6 RA-Guard July 2008

[reference2]
KAME Project, "rafixd - developed at KAME - An active rogue RA nullifier (<http://www.kame.net/dev/cvsweb2.cgi/kame/kame/kame/rafixd/>)", November 2007.

[reference3]
Hagino (itojun), Jun-ichiro., "Discussion of the various solutions (<http://ipv6samurais.com/ipv6samurais/>)"

[demystified/rogue-RA.html](#))", 2007.

Authors' Addresses

Gunter Van de Velde
Cisco Systems
De Kleetlaan 6a
Diegem 1831
Belgium

Phone: +32 2704 5473
Email: gunter@cisco.com

Eric Levy Abegnoli
Cisco Systems
Village d'Entreprises Green Side - 400, Avenue Roumanille
Biot - Sophia Antipolis, PROVENCE-ALPES-COTE D'AZUR 06410
France

Phone: +33 49 723 2620
Email: elevyabe@cisco.com

Ciprian Popoviciu
Cisco Systems
7025-6 Kit Creek Road
Research Triangle Park, North Carolina NC 27709-4987
USA

Phone: +1 919 392-3723
Email: cpopovic@cisco.com

NIIF/Hungarnet
18-22 Victor Hugo
Budapest H-1132
Hungary

Phone: tbc
Email: mohacsi@niif.hu

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

