v6ops Working Group
Internet-Draft
Expires: July 31, 2008

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

January 28, 2008

IPv6 RA-Guard
<draft-vandevelde-v6ops-ra-guard-01.txt>

Abstract

When using IPv6 within a single L2 network segment it is neccesary to ensure that all routers advertising their services within it are valid. In cases where it is not convinient or possible to use SeND [1] a rogue Router Advertisement (RA) [2] could be sent by accident due to misconfiguraton or ill intended. Simple solutions for

protecting against rogue RAs are beneficial in complementing SeND in securing the L2 domain for ceratin types of devices or in certain transitional situations.

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

When operating IPv6 in a shared L2 network segment without complete SeND support by all devices connected or without the availability of the infrastructure neccesary to support SeND, there is always the risk of facing operational problems due to rogue Router Advertisements generated malliciously or unintentionaly 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 [3] [4] [5].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 untill 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 intends to provide simple solutions to the rogue-RA problem in such contexts and while in some cases it will do that through a simple solution, in others it leverages SEND between capable devices (L2 and routers) to provide protection to devices that do not consistently use SEND.

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.

Depending on the mode of operation, 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 advertisments 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 decission 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 the L2 switch 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 decides whether the analyzed RAs should be forwarded or blocked. Based on this decission, 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 mesages 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 mecahnism 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

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

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

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

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

[5] 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

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

Phone: tbc
Email: mohacsi@niif.hu

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).