Internet Engineering Task Force (IETF)
Request for Comments: 6105
Category: Informational
ISSN: 2070-1721

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

February 2011

IPv6 Router Advertisement Guard

Abstract

Routed protocols are often susceptible to spoof attacks. The canonical solution for IPv6 is Secure Neighbor Discovery (SEND), a solution that is non-trivial to deploy. This document proposes a light-weight alternative and complement to SEND based on filtering in the layer-2 network fabric, using a variety of filtering criteria, including, for example, SEND status.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6105.

Table of Contents

1. Introduction

When operating IPv6 in a shared layer-2 (L2) network segment without complete SEcure Neighbor Discovery (SEND) support by all devices connected or without the availability of the infrastructure necessary to support SEND [RFC3971], there is always the risk of facing operational problems due to rogue Router Advertisements (RAs) generated maliciously or unintentionally by unauthorized or improperly configured routers connecting to the segment.

There are several examples of work done on this topic that resulted in related studies and code, including [NDPMON] [KAME] [IPv6-SAMURAIS]. This document describes a solution framework for the rogue-RA problem [RFC6104] where network segments are designed around a single L2-switching device 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 criterion is used by the L2 device to dynamically validate or invalidate a received RA, this criterion can even be based on SEND mechanisms).

2. Model and Applicability

RA-Guard applies to an environment where all messages between IPv6 end-devices traverse the controlled L2 networking devices. It does not apply to shared media, when devices can communicate directly without going through an RA-Guard-capable L2 networking device.

Figure 1 illustrates a deployment scenario for RA-Guard.

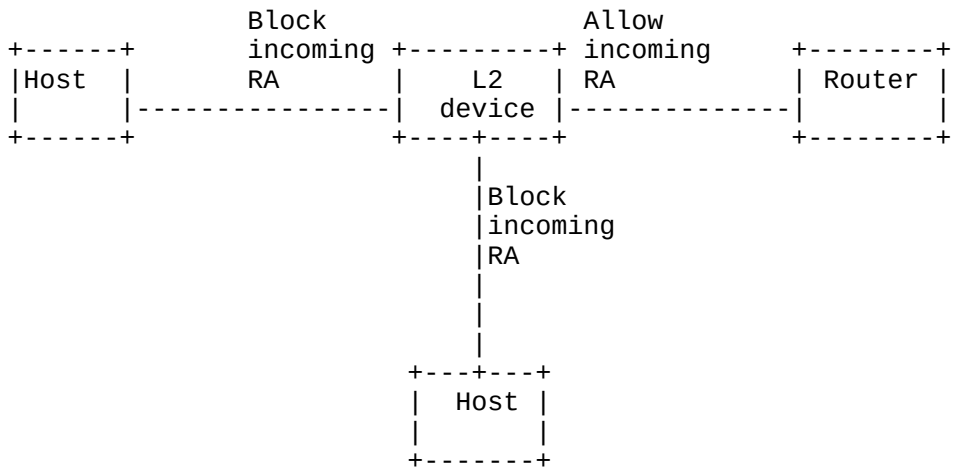

Figure 1

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, such as IPv6-enabled sensors, might not consider implementing SEND at all. An RA-Guard implementation that SEND-validates RAs 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 criteria, from a simplistic "RA disallowed on a given interface" to "RA allowed from pre-defined sources" and up to a full-fledged SEND "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 analyzing 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

[RFC4861]. If any other criterion 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 criterion and filter out any RA that does not comply. If this node-in-the-middle is an L2 device, it will not change the content of the validated RA and will 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 a context environment consisting of a mix of SEND-capable devices (L2 switches and routers) and devices that do not consistently use SEND. Furthermore, 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. Stateless RA-Guard

Stateless RA-Guard examines incoming RAs and decides whether to forward or block them based solely on information found in the message or in the L2-device configuration. Typical information available in the frames received, useful for RA validation, is as follows:

- Link-layer address of the sender
- Port on which the frame was received
- IP source address
- Prefix list

The following configuration information created on the L2 device can be made available to RA-Guard, to validate against the information found in the received RA frame:

- Allowed/Disallowed link-layer address of the RA sender
- Allowed/Disallowed ports for receiving RAs
- Allowed/Disallowed IP source addresses of the RA sender
- Allowed Prefix list and Prefix ranges
- Router Priority

Once the L2 device has validated the content of the RA frame against the configuration, it forwards the RA to its destination, whether unicast or multicast. Otherwise, the RA is dropped.

An example of a very simple stateless RA-Guard implementation could be a small L2 switch for which there is one interface "statically configured" as the interface connecting to a router, while all other interfaces are for non-router devices. With this small static setup, the only interface forwarding RAs will be the pre-assigned router interface, while the non-router interfaces block all RAs.

4. Stateful RA-Guard

4.1. State Machine

Stateful RA-Guard learns dynamically about legitimate RA senders and stores this information for allowing subsequent RAs. A simple stateful scheme would be for the L2 device to listen to RAs during a certain manually configured period of time, where the start of the listening period and the duration of the listening period for a single instance are controlled by the manual intervention. As a result, the L2 device can then allow subsequent RAs only on those ports on which valid RAs were received during this period. Often, the "LEARNING" state will only be activated by manual configuration when a new IPv6 router is provisioned on the L2 network.

A more sophisticated stateful scheme is based on SEND and is described in Section 4.2.

The state machine for stateful RA-Guard can be global, per-interface, or per-peer, depending on the scheme used for authorizing RAs.

When RA-Guard is SEND-based, the state machine is per-peer and defined in [RFC3971].

When RA-Guard is using a discovery method, the state machine of the RA-Guard capability consists of four different states:

- State 1: OFF

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

- State 2: LEARNING

  A device or interface in the RA-Guard "LEARNING" state is actively acquiring information about the IPv6 routing devices connected to its interfaces. The learning process takes place over a pre-defined unique period of time, as set by manual configuration;

or it can be event-triggered. The information gathered is compared against pre-defined criteria (criteria similar to the stateless RA-Guard rules) to 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 "all" of the RAs until their validity is verified.

When the L2 device reaches the end of the LEARNING state, it has a record of which interfaces are attached to links with valid IPv6 routers. The L2 device transitions each interface from the LEARNING state into either the BLOCKING state if there was no valid IPv6 router discovered at the interface, or into the FORWARDING state if there was a valid IPv6 router discovered.

- State 3: BLOCKING

  A device or interface running RA-Guard and in the BLOCKING state will block ingress RA messages.

  An interface can transition from the BLOCKING state into the FORWARDING state directly if explicitly instructed by the L2-device operator.

  An interface can transition from the BLOCKING state into the LEARNING state if either explicitly instructed by the L2-device operator or prompted by a triggered event.

- State 4: FORWARDING

  A device or interface running RA-Guard and in the FORWARDING state will accept valid ingress RAs and forward them to their destination.

  An interface can transition from the FORWARDING state into the BLOCKING state directly if explicitly instructed by the L2-device operator.

  An interface can transition from the FORWARDING state into the LEARNING state if either explicitly instructed by the L2-device operator or prompted by a triggered event.

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

4.2. SEND-Based RA-Guard

In this scenario, the L2 device is blocking or forwarding RAs based on SEND considerations. Upon capturing an RA on the interface, the L2 device will first verify the Cryptographically Generated Address (CGA) [RFC3971] and the RSA (Rivest, Shamir, and Adleman algorithm for public-key cryptography) signature, as specified in Section 5 of [RFC3971]. The RA should be dropped in case of failure of this verification. It will then apply host behavior as described in Section 6.4.6 of [RFC3971]. In particular, the L2 device will attempt to retrieve a valid certificate from its cache for the public key referred to in the RA. If such a certificate is found, the L2 device will forward the RA to its destination. If not, the L2 device will generate a Certification Path Solicitation (CPS) [RFC3971] with an unspecified source address, to query the router certificate(s). It will then capture the Certification Path Advertisement (CPA) [RFC3971] and attempt to validate the certificate chain. Failure to validate the chain will result in dropping the RA. Upon validation success, the L2 device will forward the RA to its destination and store the router certificate in its cache.

In order to operate in this scenario, the L2 device should be provisioned with a trust anchor certificate, as specified in Section 6 of [RFC3971]. It may also establish layer-3 connectivity with a Certificate Revocation List (CRL) Certification Path Advertisement server and/or with an NTP server. A bootstrapping issue in this case can be resolved by using the configuration method to specify a trusted port to a first router, and the SEND-based RA-Guard method on all other ports. The first router can then be used for Network Time Protocol (NTP) [RFC5905] and CRL connectivity.

5. RA-Guard Use Considerations

The RA-Guard mechanism is effective only when all messages between IPv6 devices in the target environment traverse controlled L2 networking devices. In the case of environments such as Ethernet hubs, devices can communicate directly without going through an RA-Guard-capable L2 networking device, and the RA-Guard feature cannot protect against rogue RAs.

RA-Guard mechanisms do not offer protection in environments where IPv6 traffic is tunneled.

6. Security Considerations

Once RA-Guard has set up the proper criteria (for example, it specified that a port is allowed to receive RAs, or it identified legitimate sources of RAs or certificate bases [RFC4861]), then there are no possible instances of accidentally filtered legitimate Router Advertisements, assuming the RA-Guard filter enforcement strictly follows the RA-Guard set criteria.

In Section 4.1, a simple mechanism to dynamically learn the valid IPv6 routers connected to an L2 device is explained. It is important that this LEARNING state is only entered intentionally by manual configuration. The list of learned IPv6 routers should be verified by the network manager to make sure that it corresponds with the expected valid RA list. This procedure will make sure that either accidentally or intentionally generated rogue RAs are blocked by RA-Guard.

7. Acknowledgements

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

8. References

8.1. Normative References

[RFC3971] Arkko, J., Ed., 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.

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

8.2. Informative References

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

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

[IPv6-SAMURAIS]
Hagino (itojun), J., "IPv6 demystified: I have a problem with rogue RAs in my IPv6 network", 2007, <http://ipv6samurais.com/>.

[RFC6104] Chown, T. and S. Venaas, "Rogue IPv6 Router Advertisement Problem Statement", RFC 6104, February 2011.

Authors' Addresses

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

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

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

Ciprian Popoviciu
Technodyne
111 Wood Ave. S.
Iselin, NJ 08830
USA

Phone: +1 1 919 599-5666
EMail: chip@technodyne.com

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

EMail: mohacsi@niif.hu