Network Working Group
Internet-Draft
Intended status: Experimental
Expires: November 23, 2013

P. Pfister
A. Petrescu
CEA

July 29, 2013

Routers auto-configuration using Route Information Option from ICMPv6 Router Advertisements
draft-pfister-moving-net-autoconf-00

Abstract

This draft defines a way for multiple routers that are communicating on a single link to exchange routing information using Router Advertisements. This allows moving networks to communicate with each other through auto-configured routers. This document specifies a new flag for the Router Information option from ICMPv6 Router Advertisement messages and specifies how routers must process such options.

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 November 23, 2013.

Copyright Notice

Copyright (c) 2013 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 the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction and motivations

The Neighbor Discovery protocol [NEIGHDISC] enables auto-configuration for hosts based on information provided by routers (in Router Advertisements). It assumes routers to be access routers, advertising different on-link prefixes and providing access to the whole network, and thus mainly focuses on the last hop of networks.

More specific options also exist in order to provide complementary informations for more complex and dynamic networks. For example, ICMPv6 Router Advertisements can carry DNS configuration information [RADNS] or more specific route information [RIO].

The Neighbor Discovery protocol well succeeds in configuring mobile hosts when visiting fixed networks served by fixed routers, but doesn't allow moving networks, served by an attached moving router, to interact with fixed or moving networks.

This draft extends the Neighbor Discovery protocol. It defines a new flag for the Route Information Option from [RIO] and specifies routers processing of such options when the flag is set. Thus allowing moving networks to dynamically use routing information in a simpler and more dynamic way than existing routing protocols. Finally, we discuss the different possibilities of securing such process.

2. Terminology

This document uses the terminology defined in [NEIGHDISC], and [RIO].

3. Requirements

The keywords MUST, MUST NOT, SHOULD, SHOULD NOT, MAY, CAN, when they appear in this document, are to be interpreted as described in [KEYWORDS].

4. Use case example

In most cases, only hosts are considered to be mobile, but with the increase in the number of IP devices, we can expect the number of moving networks to highly increase in the next few years. For example, cars will contain a lot of different devices, from pressure captors to infotainment terminals, all gathered in possibly complex networks. The neighbor discovery protocol allows such devices to dynamically obtain their needed networking information, but routers that serves such networks cannot use this protocol to establish connexions with the infrastructure or other cars.

This draft proposes to extend the Route Information option (RIO) use-case by allowing moving networks, that share a common link, to exchange routing information, and thus form multiple hops networks.

The simplest example of such a situation happens when two routers, configured as default gateways for fixed networks, connect to the same link. This draft allows them to advertise their respective prefixes on the visited link.

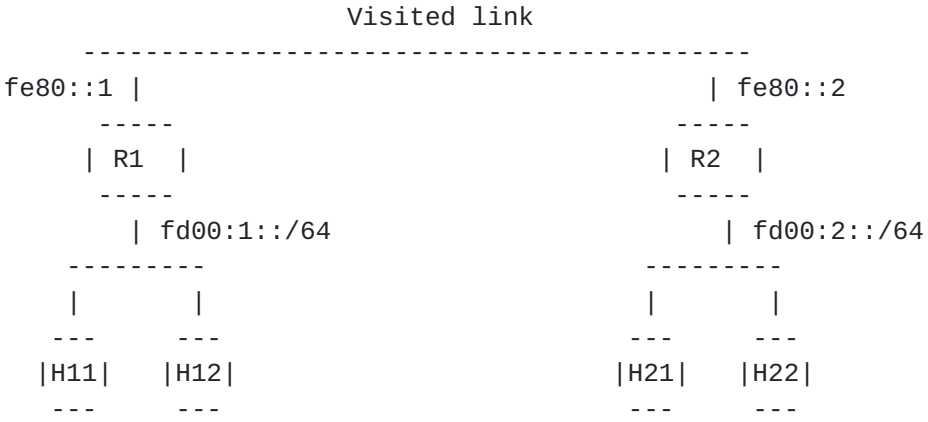
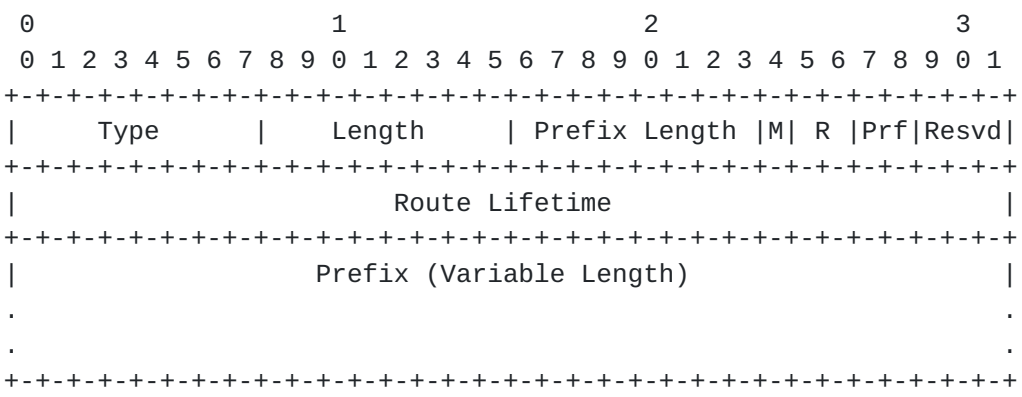


Figure 1: Two moving networks auto-configuration

In this figure, two 1-hop networks, served by their respective default routers, come in communication range on a visited link. This draft proposes a simplified procedure for those routers to exchange their internal prefixes (fd00:1::/64 and fd00:2::/64), thus allowing leaf nodes from one network (H11 and H12) to communicate with the nodes in the other network (H21 and H22).

5. Message Format

The RIO is defined in [RIO] as a Router Advertisement option. It is used by routers to send preference information about specific routes that hosts can take into account in their route selection process. This document proposes to reserve the bit 24 for Mobile Network Prefix flag.



'M': Mobile Network Prefix flag. It MUST be set to 1 if this Route Information option can be used by a router and set to 0 otherwise.

'R': Two reserved bits. They MUST be initialized to zero by the sender and ignored by the receiver.

A router sets the 'M' flag when it wants receiving routers to modify their routing table in order to use itself as next hop for the specified prefix, with the specified preference. If the flag is set, a router MAY use this information in order to modify its routing table. If not, it SHOULD ignore the option. In both cases, a host MUST behave as specified in [RIO].

6. Host Specifications

[RIO] defines three different kind of valid behaviors for hosts. This document doesn't propose any modification for hosts. Therefore, a host MUST ignore the Mobile Network Prefix flag.

7. Router Specifications

7.1. Router configuration

Routers SHOULD NOT set the Mobile Network Prefix flag by default in the Route Information options they send but they SHOULD be configureable.

The default behavior of router MUST be to ignore all received Route Information options. But a router SHOULD be configurable in order to specify other behaviors.

7.2. Accepting a Route Information option

Routers SHOULD ignore all Route Information option which Mobile Network Prefix flag is not set. When the flag is set, a router submits the option to its acceptation algorithm in order to decide whether to accept the RIO or not.

Routers MAY accept all, none, or some of the RIOs which 'M' flag is set. Such selection CAN be based on any kind of policy (source address, authentication, etc...).

7.3. Using a Route Information option

When accepted, a RIO is used as defined in [RIO] for type C hosts. The receiving router is free to give any metric to the newly introduced route.

When routing a packet, longest prefix match is first used. When different next-hops addresses exist for the same packet, with the same metric, routes that are obtained through Route Information options have the lowest priority. The preference field is used in order to break ties between routes that were obtained with RIOs.

Routing entries that are obtained with RIOs MUST be removed after at most 'Route lifetime' seconds unless its lifetime is extended by a newly received RIO from the same neighbor. If so, the new preference value and timeout date override previously received values.

8. Security Considerations

The Neighbor Discovery protocol have some known security weaknesses. This draft doesn't intend to solve them. Nevertheless, route auto-configuration for routers extends the scope of possible threats from a single node to a complete network. Special care should therefore be taken when deciding whether to accept or reject a Route Information option.

8.1. Using IPSec

IPSec [IPSEC] can be used, in some cases, to secure the Neighbor Discovery messages. But, as it only supports security associations between pairs of nodes, it requires unicast communications. Care should therefore be taken when considering this solution in order to avoid congestion.

8.2. Using SeND

SeND [SEND] uses public-key cryptography in order to broadcast signed Router Advertisements. X.509 certificates are used in order to certify the right of routers to advertise a set of prefixes. This document proposes to extends the right of advertising a prefix (in Prefix Information options) to the right of advertising the same prefixes in RIOs.

In other words, when SeND is enabled, a router MUST NOT send RIOs containing prefixes it hasn't the right to send in Prefix Information options.

The use of this protocol would not prevent a malicious node, present on the shared link, to spoof IPs from both networks, to eaves-drop, or potentially to perform man-in-the-middle attacks, depending on the shared link security. Connected networks should therefore use higher layers security in order to establish point-to-point secured connexions.

9. IANA Considerations

IANA is kindly requested by the authors to allocate the following value:

- Space allocation for the Mobile Network Prefix flag in the Route Information option.

10. Acknowledgements

11. References

[KEYWORDS] Bradner, S., "Key words for use in RFCs to indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[RIO] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, November 2005.

[RADNS] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 6106, November 2010.

[IPSEC] Loughney, J., "IPv6 Node Requirements", RFC 4294, April 2006.

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

Authors' Addresses

Pierre Pfister
Commissariat a l'Energie Atomique
8 Avenue de la Vauve
Palaiseau, Ile-de-France 91120
FR

Email: pierre.pfister@polytechnique.org

Alexandru Petrescu
Commissariat a l'Energie Atomique
8 Avenue de la Vauve
Palaiseau, Ile-de-France 91120
FR

Email: alexandru.petrescu@cea.fr