Network Working Group
Internet Draft
Intended status: Stand Track
Expires: April 30, 2015

B. Liu
Huawei Technologies

October 27, 2014

IPv6 ND Option for Network Management Server Discovery
draft-liu-6man-nd-nms-discovery-01.txt

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 April 30, 2015.

Copyright Notice

Abstract

This document introduces a mechanism for devices to actively learn the NMS server address from the neighbors through IPv6 ND protocol extension. It is a good leverage of IPv6 automatic features.

This document only discusses problem/solution within the IPv6-only networks/plane.

Table of Contents

1. Introduction

NMS (Network Management System) has become a must-have component in modern networks. It could be utilized to benefit various aspects of a network. For example, the emerging router auto-configuration solutions are mostly based on NMS. If the devices could successfully connect to the NMS server(s), then auto-configuration won't be a problem.

So there is a key problem of how to discover the NMS server for the devices when they get online. Currently there are mainly two methods to solve the problem. One is to set the NMS server's IP/URL into the devices before shipping to the customer premises; the other one is the NMS actively discovering the devices through some polling mechanisms. The former one is easy to be implemented and deployed, but it lacks flexibility due to the static pre-configuration and might be error-prone for configuration when the different networks have different NMS servers; the latter one lacks the instantaneity due to the polling mechanisms need the intermediate nodes to integrate supporting features which introduce complex functions and protocols.

This document introduces a mechanism for devices to actively learn the NMS server from the neighbors through IPv6 ND protocol extension. It is a good leverage of IPv6 automatic features.

This document only discusses problem/solution within the IPv6-only scope.

2. Basic Approach

When a device gets online, we could assume that its neighbors who have already got online have learnt the NMS server's address. So it is quite easy for the new device to learn the information from its neighbor.

This document is based on the above Neighbor-Learning approach.

3. Scenario Description

3.1. New Devices Getting Online

- Adding a New Device into an Existing Network

For adding a new device into an existing network, it is very reasonable to assume that the neighbors have already connected to the NMS server. So it is obvious that the new device could easily learn the NMS server's address from neighbors.

- Deploying a New Network

In the case of deploying a new network, the NMS server address needs to be propagated to the whole network, then some kind of flooding mechanism is needed if the propagation also relies on above mentioned neighbor-learning approach. This is applicable through careful plan which might need proper order for the devices to get online successively.

The detail of the flooding mechanism is out of the scope of this document. We treat it as an assumption for the application of neighbor-learning NMS discovery.

3.2. Regarding Connectivity

- Connecting NMS after Getting Global Connectivity

Normally, address assignment is not coupled with NMS processing. Before connected to the NMS server, the devices could obtain global connectivity either through SLAAC or DHCPv6.

In this case, once the devices have learnt the NMS server address, they could directly connect to get more configurations.

- Connecting NMS before Getting Global Connectivity

In contrast, address assignment might be done through NMS in some situations. For example, the device is a backbone router, and the address has been carefully planned and pre-configured in the NMS server, when the device connect to the server, it will be assigned global address through network management processing.

In this case, after learning the NMS server address, the device might need a proxy to communicate with the server or configuring itself a ULA address and utilizing the NPTv6 processing on its neighbor or uplink router. The details are out of the scope of this document.

4. Neighbor Discovery Extension for Supporting NMS Discovery

Since ND is a basic protocol in IPv6, every router supports IPv6 would support ND, we utilize ND extension to achieve the above mentioned neighbor-learning NMS server discovery.

4.1. Option Definition

This section introduces a new option defined to carry the NMS address in ND messages.

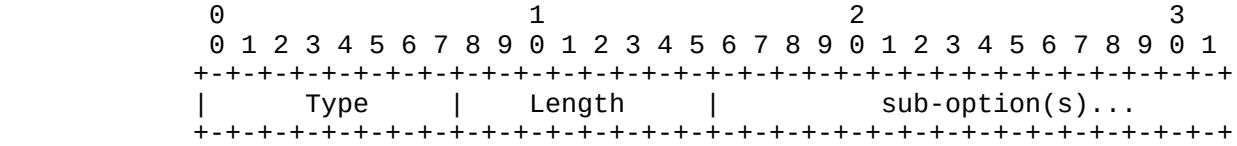

Figure 1: Neighbor Discovery NMS Discovery Option

o Type: TBD (to be assigned by IANA)

o Length: The length of the option (including the type and length fields) in units of 8 octets.

o sub-option(s): using sub-option(s) to allow multiple formats of the NMS server location. Sub-option(s) are defined as the following Section 4.2.

4.2. Sub-Options Definition

To support multiple NMS server location formats, three sub-options are defined as the following.

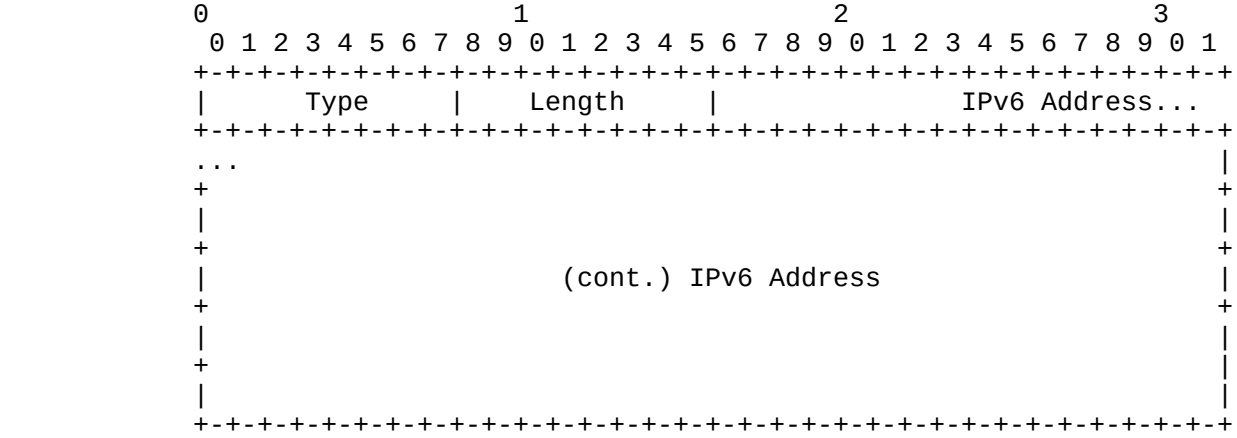

Figure 2: IPv6-Address Sub-option of NMS Server Location

o Type: TBD (to be assigned by IANA)

o Length: 3

o IPv6 Address: 128bit IPv6 address with zero padding behind

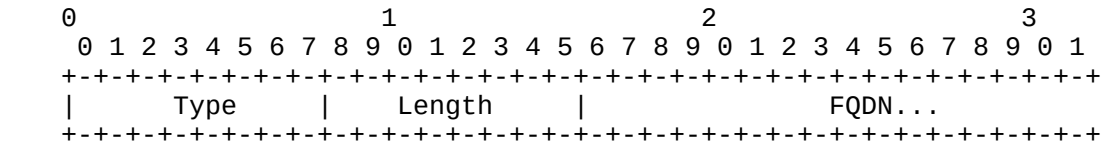

Figure 3: FQDN Sub-option of NMS Server Location

o Type: TBD (to be assigned by IANA)

o Length: The length of the option (including the type and length fields) in units of 8 octets.

o FQDN: FQDN of the NMS server, variable length

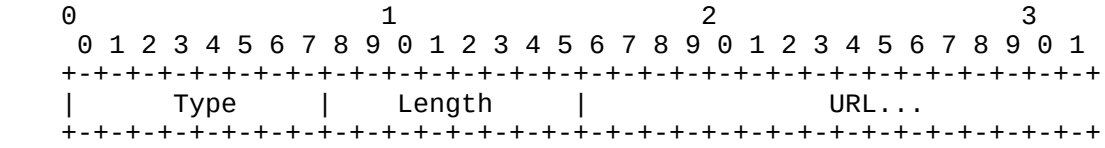

Figure 3: FQDN Sub-option of NMS Server Location

o Type: TBD (to be assigned by IANA)

o Length: The length of the option (including the type and length fields) in units of 8 octets.

o URL: URL of the NMS server, variable length

4.3. Option Carried in Router Advertisement Messages

- RA-only Mode

A device discoveries NMS server’s address through received Router Advertisement messages which include a new option defined for carrying NMS server’s address.

Since RA messages are usually generated by the gateway on a link, this approach is suitable for a hub-and-spoke subnet in which a new device joins in.

After having learnt the NMS server’s address, then the device could directly connect to the server

4.4. Option Carried in Neighbor Solicit/Advertisement Messages

A device discoveries NMS server’s address through actively initiating Neighbor Solicit message and receiving Neighbor Advertisement messages which include the new option carrying the NMS server’s address.

This approach is suitable for point-to-point or non-broad circuits.

5. Security Considerations

- Device authentication for NMS Servers

With applying the mechanism described in this document, the devices would actively connect to the NMS servers. So there might be stronger desire for the NMS servers to authenticate the devices.

- ND security

This document doesn’t introduce more threats than original Neighbor Discovery protocol, so generally it aligns with the security considerations described in [RFC4861].

6. IANA Considerations

The newly defined options need IANA to assign type codes.

7. Acknowledgments

Many useful comments and contributions were made by Sheng Jiang.

8. References

8.1. Normative References

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

Authors' Addresses

Bing Liu
Huawei Technologies Co., Ltd
Q14, Huawei Campus
No.156 Beiqing Rd.
Hai-Dian District, Beijing 100095
P.R. China

Email: leo.liubing@huawei.com