

INTERNET-DRAFT  
Intended Status: Standard Track  
Expires: September 8, 2011

B.Liu  
S.Jiang  
Huawei Technologies Co., Ltd  
March 7, 2011

**SLAAC/DHCPv6 conflicts diagnostic during site renumbering  
draft-liu-ipv6-renum-conflicts-00.txt**

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [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/lid-abstracts.html>

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

Copyright and License Notice

Copyright (c) 2011 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.

## Abstract

While an IPv6 site is being renumbered, both DHCPv6 and ND may be used to reconfigure the host addresses. This may cause potential address configuration conflicts during renumbering procedure. The issue mainly include two situations: a) Address configuration method conflict, which means a host receives a new prefix comes from another address configuration protocol. b) Address prefix conflict, a host receives both DHCPv6 and ND address configuration messages which assign different address prefixes. This documents analyzes the conflict issues and proposes a conflict report mechanism for hosts to report the conflicts to DHCPv6 servers.

## Table of Contents

<a href="#">1</a>	<a href="#">Introduction</a>	<a href="#">3</a>
<a href="#">1.1</a>	<a href="#">IPv6 renumbering</a>	<a href="#">3</a>
<a href="#">1.2</a>	<a href="#">DHCPv6/ND address configuration conflict</a>	<a href="#">3</a>
<a href="#">2</a>	<a href="#">Terminolog</a>	<a href="#">5</a>
<a href="#">3</a>	<a href="#">Conflict Report Mechanism</a>	<a href="#">5</a>
<a href="#">3.1</a>	<a href="#">Host behavior</a>	<a href="#">5</a>
<a href="#">3.2</a>	<a href="#">Conflict Report Trigger</a>	<a href="#">5</a>
<a href="#">3.3</a>	<a href="#">DHCPv6 Reconfiguration Conflict Options</a>	<a href="#">6</a>
<a href="#">3.4</a>	<a href="#">Report processing by DHCPv6 server</a>	<a href="#">6</a>
<a href="#">4</a>	<a href="#">Security Considerations</a>	<a href="#">7</a>
<a href="#">5</a>	<a href="#">IANA Considerations</a>	<a href="#">7</a>
<a href="#">6</a>	<a href="#">Acknowledgements</a>	<a href="#">7</a>
<a href="#">7</a>	<a href="#">References</a>	<a href="#">7</a>
<a href="#">7.1</a>	<a href="#">Normative References</a>	<a href="#">7</a>
<a href="#">7.2</a>	<a href="#">Informative References</a>	<a href="#">7</a>
	<a href="#">Author's Addresses</a>	<a href="#">8</a>



## **1 Introduction**

### **1.1 IPv6 renumbering**

"Renumbering" is an event of changing in IP addressing information associated with a host or subnet [[RFC1900](#)]. [[RFC5887](#)] and [[I-D.chown-v6ops-renumber-thinkabout](#)] described numerous reasons why such sites might need to renumber in a planned fashion, for example, change of site topology, change of service provider etc.

[RFC4192] provided a general procedure of renumbering in an IPv6 network, which is achieved by changing address prefix. Before the old prefix is withdrawn, the hosts are assigned a new prefix. Both the old and the new prefixes may be usable till the new prefix is stable in the site systems, such as DNS, ACL .etc. Then the old prefix will be withdrawn. The transition periods are variable according to different network management settings.

[RFC4192] also mentioned several methods to reconfigure addresses while renumbering:

- o Stateful address configuration through Dynamic Host Configuration Protocol for IPv6 (DHCPv6) protocol [[RFC3315](#)]
- o Stateless address configuration through Neighbor Discovery Protocol[RFC4861] (SLAAC) [[RFC4862](#)]
- o Manual configuration

This document focuses on the address reconfiguration problem and there is a specific issue of IPv6 site renumbering described as the following.

### **1.2 DHCPv6/ND address configuration conflict**

Both of the DHCPv6 and ND protocols have IP address configuration function. They are suitable for different scenarios respectively. During renumbering, the SLAAC-configured hosts can reconfigure IP addresses by receiving ND Router Advertisement (RA) messages containing new prefix information. The DHCPv6-configured hosts can reconfigure addresses by initialing RENEW sessions when the current addresses' lease time is expired or receiving the reconfiguration messages initialed by the DHCPv6 servers.

But DHCPv6 and ND address configuration may overlap and cause conflict on a host. The issue includes two situations:

- A DHCPv6-configured host receives RA messages containing new



## prefix

Ideally, hosts in a DHCPv6-managed network should not receive any ND address configuration messages to avoid potential confusion. But some factors may cause this happen. For example, a sub-net of a DHCPv6-managed network may be mis-configured to use SLAAC for address configuration; or a DHCPv6-managed network contains hosts (some specific types of Apple Mac computers, e.g.) that don't support DHCPv6 as the default so that SLAAC will be used along with DHCPv6 as a necessary supplement.

There are no standards specifying what approach should be taken by a DHCPv6-configured host when it receives RA messages containing new prefix. It depends on the operation system of the host and cannot be predicted or controlled by the network. If the host accepts the new prefix in RA, it may violate the DHCPv6-managed policies. But if it ignores the RA messages and there are no DHCPv6 reconfiguration messages received either, the renumbering would fail. What is worse, the host may even receive both the RA messages and DHCPv6 reconfiguration messages and finds the prefixes in the two protocols are different. This means serious network configuration error occurring.

- A SLAAC-configured finds DHCPv6 is in use

[RFC5887] and [[I-D.jiang-ipv6-site-renum-guideline](#)] mentioned RA message of ND protocol contains a "Managed Configuration" flag to indicate DHCPv6 is in use. But it is unspecified what behavior should be taken when the host receives RA messages with "M" set to 1. The gap of standard will cause ambiguous host behavior because it depends on the operation system of the host.

The host may start a DHCPv6 session and receives the DHCPv6 address configuration. It is also possible that the host finds the DHCPv6 assigned prefix is different from the prefix in the RA messages, which means there is a serious network configuration error.

Another possibility is that the host may receive no response from any DHCPv6 servers, which means the DHCPv6 service is not available and the "Managed Configuration" flag was mis-configured.

These potential conflicts described above need to be addressed. This document proposes a report mechanism for hosts to report the conflicts to DHCPv6 servers. (The mis-configured "Managed Configuration" flag issue described above is not addressed in this document because there are no DHCPv6 servers available in that circumstance. Whether it needs to report the conflict to routers or some other servers such as network management systems needs further



study.)

## **[2](#) Terminolog**

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

## **[3](#) Conflict Report Mechanism**

As analyzed above, while renumbering, hosts received address configuration messages (either ND or DHCP protocol messages), if the messages conflict with existing/previous configuration mechanism, hosts report address configuration policy conflict information to the network. And then they accept the address configuration indication from the network.

The conflicts can be outlined as two types:

- Prefix conflict, which means prefixes in DHCPv6 and ND messages are different.
- Address configuration method conflict, which means a host receives a new prefix comes from another address configuration protocol.

There are several approaches of the mechanism as the following clauses.

### **[3.1](#) Host behavior**

For the DHCPv6-configured hosts, it assumes that they will monitor the RA messages after being configured by DHCPv6.

For the SLAAC-configured hosts, it assumes that the hosts initially explored the DHCPv6 servers based on having already chosen DHCPv6 as high priority of address configuration protocol when it finds the "Managed Configuration" flag is set.

### **[3.2](#) Conflict Report Trigger**

Rules for the hosts to trigger conflict reports are as the following:

- Prefix conflict trigger, a host will trigger the report when it finds the prefixes are different in DHCPv6 and ND messages.





- Address configuration method conflict trigger, a DHCPv6-managed host receives a new prefix comes from RA messages.

### **[3.3](#) DHCPv6 Reconfiguration Conflict Options**

New DHCPv6 options could be defined respectively for the clients to report conflicts to servers and for servers to response according to analysis of the reported conflict details.

- Option\_ReconfigConflict\_Report

It is possible to include this option into the renew message. The content of the option could be:

- a) New available address prefix (prefix in RA e.g.).
- b) Serious error of prefix conflict.

- Option\_ReconfigConflict\_Response

DHCPv6 server could response as the following possibilities according to information got from the option:

- a) Directly assigns new addresses to the hosts who report conflicts.
- b) Indicates hosts to make SLAAC according to RA messages received.
- c) Report the prefixes conflict to network management system.

### **[3.4](#) Report processing by DHCPv6 server**

When a DHCPv6 server receives the conflict reports, it should analyze the report and decides whether to forward the report to relative network management systems or indicate what approach should be taken to the hosts through DHCPv6 messages defined in [section 3.3](#), however, the analysis processing of DHCPv6 servers is not in the scope of this memo.



## **4 Security Considerations**

This document doesn't provide additional security considerations for IPv6 site renumbering more than [[RFC5887](#)], [[RFC4192](#)] and other relative documents.

For the conflict report mechanism, there is a potential threat that any malicious host can fake conflict reports to DHCPv6 servers which may disturb the network manager when the report is prefix conflict, however, it cannot directly break the availability of the network.

## **5 IANA Considerations**

This document requests IANA to assign new DHCPv6 option number.(TBD)

## **6 Acknowledgements**

This document inherits various previous work. Thanks for Brian Carpenter, Randall Atkinson, Hannu Flinck, Fred Baker, Eliot Lear, Ralph Droms, Tim J. Chown, Mark K. Thompson, Alan Ford, and Stig Venaas.

## **7 References**

### **7.1 Normative References**

- [RFC3315] R. Droms, Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6(DHCPv6)", [RFC 3315](#), July 2003.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.
- [[RFC4862](#)] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [RFC 4862](#), September 2007.

### **7.2 Informative References**

- [RFC5887] Carpenter, B., Atkinson, R., and H. Flinck, "Renumbering Still Needs Work", [RFC 5887](#), May 2010.
- [RFC4192] Baker, F., Lear, E., and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", [RFC 4192](#), September 2005.
- [I-D.jiang-ipv6-site-renum-guideline]  
Jiang, S., and Liu B., "IPv6 Site Renumbering Guidelines



and Further Works", working in progress.

[I-D.chown-v6ops-renumber-thinkabout]

Chown, T., and Thompson, M., "Things to think about when  
Renumbering an IPv6 network", September 2006.

#### Author's Addresses

Bing Liu  
Huawei Technologies Co., Ltd  
Huawei Building, No.3 Xinxu Rd.,  
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085  
P.R. China  
Email: leo.liubing@huawei.com

Sheng Jiang  
Huawei Technologies Co., Ltd  
Huawei Building, No.3 Xinxu Rd.,  
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085  
P.R. China  
Email: jiangsheng@huawei.com

