

Network Working Group

Internet Draft

Intended status: Best Current Practice

Expires: January 03, 2012

S. Jiang

B. Liu

Huawei Technologies Co., Ltd

B. Carpenter

University of Auckland

July 01, 2011

IPv6 Enterprise Network Renumbering Scenarios and Guidelines  
draft-jiang-6renum-enterprise-00.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 January 03, 2012.

Copyright 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

This document analyzes the enterprise renumbering events and gives the recommendations among the existing renumbering mechanisms. According to the different stages of renumbering events,

considerations and best current recommendations are described in three categories: during network design, for preparation of renumbering, and during renumbering operation. A gap inventory is listed at the end of this document.

#### Table of Contents

1. Introduction .....	3
2. Enterprise Network Illustration for Renumbering .....	3
3. Enterprise Network Renumbering Scenario Categories .....	4
3.1. Renumbering caused by External Network Factors.....	4
3.2. Renumbering caused by Internal Network Factors.....	5
4. Network Renumbering Considerations and Best Current Recommendations .....	5
4.1. Considerations and Recommendations during Network Design.	6
4.2. Considerations and Recommendations for the Preparation of Renumbering .....	8
4.3. Considerations and Recommendations during Renumbering Operation .....	9
5. Gap Inventory .....	11
6. Security Considerations .....	12
7. IANA Considerations .....	12
8. Acknowledgements .....	12
9. Change Log [RFC Editor please remove] .....	12
10. References .....	13
10.1. Normative References .....	13
10.2. Informative References .....	14
Author's Addresses .....	15

## 1. Introduction

IPv6 site renumbering is considered difficult. Network managers would turn to Provider Independent (PI) addressing for IPv6 to attempt to minimize the need for future renumbering. However, widespread use of PI may create very serious BGP4 scaling problems. It is thus desirable to develop tools and practices that may make renumbering a simpler process to reduce demand for IPv6 PI space.

This document undertakes scenario descriptions, including documentation of current capability inventories and existing BCPs, for enterprise networks. It takes the analysis conclusions from [RFC5887] and other relevant documents as the primary input.

This document focuses on IPv6 only, by leaving IPv4 out of scope. Dual-stack network or IPv4/IPv6 transition scenarios are out of scope, too.

According to the different stages of renumbering events, considerations and best current recommendations are described in three categories: during network design, for preparation of renumbering, and during renumbering operation. A gap inventory is listed at the end of this document.

## 2. Enterprise Network Illustration for Renumbering

The enterprise network architecture is illustrated as the figure below. From the renumbering perspective of view, these entities relevant to renumbering are highlighted.

Address reconfiguration is fulfilled either by DHCPv6 or ND protocols. Static address assignment is not considered in this version. During the renumbering event, the DNS records need to be synchronized while routing tables, ACLs and IP filtering tables in various gateways also need to be updated, too.

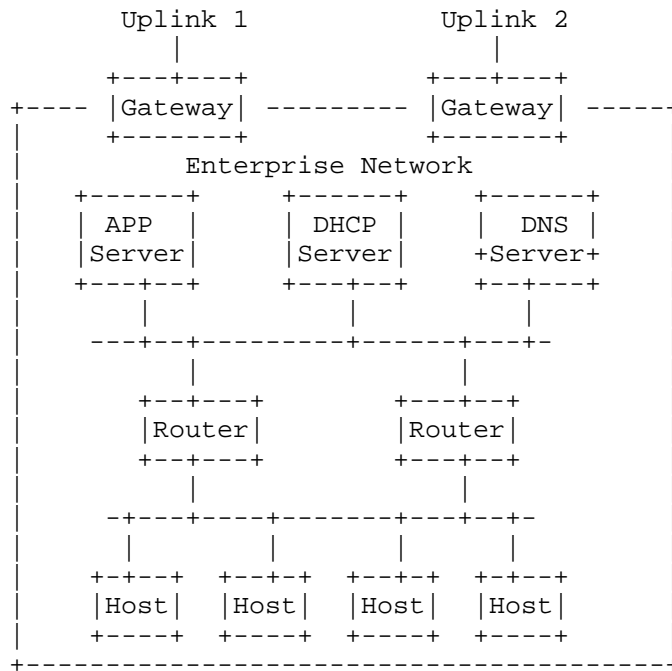


Figure 1 Enterprise network illustration

It is assumed that IPv6 enterprise networks are IPv6-only, or dual-stack in which a logical IPv6 plane is independent from IPv4. The complicated IPv4/IPv6 co-existing scenarios are out of scope.

This document focuses on the unicast addresses; site-local, link-local, multicast and anycast addresses are out of scope.

### 3. Enterprise Network Renumbering Scenario Categories

In this section, we category enterprise network renumbering scenarios mainly according to different reasons. Some of renumbering reasons described in [RFC2071] has out of date, or not suitable in IPv6, or not suitable for enterprise networks.

#### 3.1. Renumbering caused by External Network Factors

The most influential external network factor is the uplink ISP.

- o The enterprise network switches to a new ISP. Of course, the prefixes received from different ISPs are different. This is the most common scenario.

Whether there is an overlap time between the old and new ISPs would also influence the possibility whether the enterprise can fulfill renumbering without a flag day [RFC4192].

- o The renumbering event may be initiated by receiving new prefixes from the same uplink. The typical scenario is that the DHCP server in ISP delegates a new prefix to the enterprise network. Or the enterprise network may be switched to a different location within the network topology of the same ISP due to various considerations, such as commercial, performance or services reasons, etc. The ISP itself may also be renumbered due to topology change or migration to a different or additional prefix. These ISP renumbering events would initiate enterprise network renumbering events, of course.
- o The enterprise network adds new uplink(s) for multihoming purpose. This may not a typical renumbering because the original addresses will not be changed. However, initial numbering may be considered as a special renumbering event. If the administrators only want part of the network to have multiple prefixes, the renumbering process should be carefully managed.

### 3.2. Renumbering caused by Internal Network Factors

- o As companies split, merge, grow, or reorganize, the enterprise network architectures may need to be re-built. This will trigger the internal renumbering.

## 4. Network Renumbering Considerations and Best Current Recommendations

In order to carry out renumbering in an enterprise network, systematic planning and administrative preparation are needed. Carefully planning and preparation could make the renumbering process smoother.

This section tries to give the recommended solutions or strategies for the enterprise renumbering among the existing mechanisms. There are a few gaps analyzed by [I-D.liu-6renum-gap-analysis]. If they are filled in the future, the enterprise renumbering may be processed more automatically, with fewer issues.

#### 4.1. Considerations and Recommendations during Network Design

This section describes the renumbering relevant considerations or issues that a network architect should carefully plan when he builds or designs a new network.

##### - Prefix Delegation

In a large or a multi-site enterprise network, the prefix should be carefully managed, particularly during renumbering events. Prefix information needs to be delegated from router to router. The DHCPv6 Prefix Delegation options [RFC3633] provide a mechanism for automated delegation of IPv6 prefixes. DHCPv6 PD options may also be used between the enterprise routers and their upstream ISPs.

##### - Usage of FQDN

It is recommended that Fully-Qualified Domain Names (FQDNs) should be used to configure network connectivity, such as tunnels. The capability to use FQDNs as endpoint names has been standardized in several RFCs, such as [RFC5996], although many system/network administrators do not realize that it is there and works well as a way to avoid manual modification during renumbering.

Service Location Protocol [RFC2608] and multicast DNS with SRV records for service discovery can reduce the number of places that IP addresses need to be configured.

##### - Address Types

This document focuses on the dynamic-configured global unicast addresses in enterprise networks. They are the targets of renumbering events.

Manual-configured addresses are not scalable in medium to large sites, hence be out of scope. However, some hosts such as servers may need static addresses. Manual-configured addresses/hosts should be avoided as much as possible.

[Open Question to WG] What we can do regarding to manual configured hosts and static addresses, which do need to be changed?

Unique Local Address (ULA, [RFC4193]) may be used on local routers or servers, which only intends for local communications, usually

inside of enterprise networks. Normally, they do NOT need to be changed during the renumbering event.

[Open Question to WG] Is anyone actually using ULAs?

#### - Address configuration models

In IPv6 networks, there are two auto-configuration models for address assignment: the Stateless Address Auto-Configuration (SLAAC) by Neighbor Discovery (ND, [RFC4861, RFC4862]) and the stateful address configuration by Dynamic Host Configuration Protocol for IPv6 (DHCPv6, [RFC3315]). In the latest work, DHCPv6 can also support host-generate address model by assigning prefix through DHCPv6 messages [I-D.ietf-dhc-host-gen-id].

ND is considered easier to renumber by broadcasting a Router Advertisement message with a new prefix. DHCPv6 can also trigger the renumbering process by sending unicast RECONFIGURE messages though it may cause a large number of interactions between hosts and DHCPv6 server.

In principle, a network should choose only one address configuration model and employs either ND or DHCPv6. This document has no preference between ND and DHCPv6 address configuration models.

However, since DHCPv6 is also used to configure many other network parameters, there are ND and DHCPv6 co-existing scenarios. The current protocols do not effectively prevent that both SLAAC and DHCPv6 address assignment are used in the same network (see M bit analysis in section 5.1.1 [RFC5887]). It is network architects' job to make sure only one configuration model is employed. Even in a large network that contains several subnet works, it is recommended not to mix the two address configuration models though isolately using them in different subnet works may reduce the risk partly.

#### - DNS

It is recommended that the site have an automatic and systematic procedure for updating/synchronising its DNS records, including both forward and reverse mapping [RFC2874]. Manually on-demand updating model is considered as a harmful problem creator in renumbering event.

A6 DNS record model is recommended over AAAA record model for renumbering purpose [RFC2874, RFC3364].

In order to simplify the operation procedure, the network architect should combine the forward and reverse DNS updates in a single procedure.

If a small site depends on its ISP's DNS system rather than maintains its own one. When renumbering, it requires administrative coordination between the site and its ISP. Alternatively, the DNS synchronizing may be completed through the Secure Dynamic DNS Update.

#### - Security

Any automatic renumbering scheme has a potential exposure to hijacking at the moment that a new address is announced. Proper network security mechanisms should be employed. Secure Neighbor Discovery (SEND, [RFC3971]), which does not widely deployed, is recommended to replace ND. Alternatively, certain lightweight renumbering specific security mechanism may be developed in the future. DHCPv6 build-in secure mechanisms, like Secure DHCPv6 [I-D.ietf-dhc-secure-dhcpv6] or authentication of DHCPv6 messages [RFC3315] are recommended.

#### - Miscellaneous

A site or network should also avoid to embed addresses from other sites or networks in its own configuration data. Instead, the Fully-Qualified Domain Names should be used. Thusness, these connectivities can survive after renumbering events. This also applies to host-based connectivities.

### 4.2. Considerations and Recommendations for the Preparation of Renumbering

It is not possible to reduce a prefix's lifetime to below two hours. So, renumbering should not be an unplanned sudden event. This issue could only be avoided by early planning and preparation.

This session describes several recommendations for the preparation of enterprise renumbering event. By adopting these recommendations, a site could be renumbered easier. However, these recommendations are not cost free. They might increase the daily burden of network operation. Therefore, only these networks that are expected to be renumbered soon or very frequently should adopt these recommendations with the balance consideration between daily cost and renumbering cost.

- Reduce the address preferred time or valid time or both.



Long-lifetime addresses may cause issues for renumbering events. Particularly, some offline hosts may reconnect back using these addresses after renumbering events. Shorter preferred lifetime with relevant long valid lifetime may get short transition period for renumbering event and avoid address renew too frequent.

- Reduce the DNS record TTL.

The DNS record TTL on the local DNS server should be manipulated to ensure that stale addresses are not cached.

- Reduce the DNS configuration lifetime on the hosts.

Since the DNS server could be renumbered as well, the DNS configuration lifetime on the hosts should also be reduced if renumbering events are expected. The DNS configuration can be done through either ND [RFC6106] or DHCPv6 [RFC3646]. However, DHCPv6 DNS option does not include associated lifetime. It should be updated.

#### 4.3. Considerations and Recommendations during Renumbering Operation

Renumbering events are not instantaneous events. Normally, there is a transition period, in which both the old prefix and the new prefix are used in the site. Better network design and management, better pre-preparation and longer transition period are helpful to reduce the issues during renumbering operation.

- Within/without a flag day

As is described in [RFC4192], "a 'flag day' is a procedure in which the network, or a part of it, is changed during a planned outage, or suddenly, causing an outage while the network recovers."

If renumbering event is processed within a flag day, the network service/connectivity will be outage for a period till the renumbering event is completed. It is efficient and provides convenient for network operation and management. But network outage is usually unacceptable for end users and the enterprises. Renumbering procedure without a flag day provides smooth addresses switching, but much more operational complexity and difficulty is introduced.

- Transition period

If renumbering transition period is longer than all addresses lifetime, after which the addresses lease expire, each host will automatically pick up its new IP address. In this case, it would be the DHCP server or Router Advertisement itself that automatically accomplishes client renumbering.

- Network initiative enforced renumbering

If the network has to enforce renumbering before addresses lease expire, the network should initiate enforcement messages, either in Router Advertisement messages or DHCPv6 RECONFIGURE messages.

- Impact to branch/main sites

Renumbering in main/branch site may cause impact on branch/main site communication. The routes, ingress filtering of site's gateways, and DNS may need to be updated. This needs carefully planning and organizing.

- DNS record update and DNS configuration on hosts

DNS records should be updated if hosts are renumbered. If the site depends on ISP's DNS system, it should report the new host's DNS records to its ISP. During the transition period, both old and new DNS records are valid. If the TTL of DNS records is shorter than the transition period, administrative operation may not be necessary.

DNS configuration on hosts should be updated if local recursive DNS servers are renumbered. During the transition period, both old and new DNS addresses may co-exist on the hosts. If the lifetime of DNS configuration is shorter than the transition period, name resolving failure may not be reduced to minimum. A notification mechanism may be needed to indicate the hosts that a renumbering event of local recursive DNS happens or is going to take place.

- Router awareness

In a site with multiple border routers, all border routers should be aware of partial renumbering in order to correctly handle inbound packets. Internal forwarding tables need to be updated.

- Border filtering

In a multihomed site, an egress router to ISP A could normally filter packets with source addresses from other ISPs. The egress router connecting to ISP A should be notified if the egress router

connecting to ISP B initiates a renumbering event in order to properly act filter function.

- Tunnel concentrator renumbering

Tunnel concentrator itself might be renumbered. This change should be reconfigured to relevant hosts or router, unless the configuration of tunnel concentrator was based on FQDN.

## 5. Gap Inventory

This section lists a few issues that still remain unsolvable. Some of them may be inherently unsolvable.

- Manual or script-driven procedures will break the completely automatic host renumbering.
- Some environments like embedded systems might not use DHCP or SLAAC and even configuration scripts might not be an option. This creates special problems that no general-purpose solution is likely to address.
- TCP and UDP flows can't survive at renumbering event at either end.
- Some address configuration data might be widely dispersed and much harder to find, even will inevitably be found only after the renumbering event.
- The embedding of IPv6 unicast addresses into multicast addresses and the embedded-RP (Rendezvous Point) [RFC3956] will cause issues when renumbering.
- Changing the unicast source address of a multicast sender might also be an issue for receivers.
- When a renumbering event takes place, entries in the state table of tunnel concentrator that happen to contain the affected addresses will become invalid and will eventually time out. However, this can be considered as harmless though it takes sources on these devices for a while.
- A site that is listed in a black list can escape that list by renumbering itself. The site itself of course will not initiatively to report its renumbering and the black list may not be able to monitor or discover the renumbering event.

- Multihomed site, using SLAAC for one address prefix and DHCPv6 for another, would clearly create a risk of inconsistent host behaviour and operational confusion.
- The impact of portion renumbering may need to be analyzed further.

Some of these issues can be considered as harmless or have minimum impacts.

## 6. Security Considerations

A site that is listed in a black list can escape that list by renumbering itself.

Any automatic renumbering scheme has a potential exposure to hijacking at the moment that a new address is announced. Proper network security mechanisms should be employed. SEND is recommended to replace ND. Alternatively, certain lightweight renumbering specific security mechanism may be developed in the future. DHCPv6 build-in secure mechanisms, like Secure DHCPv6 [I-D.ietf-dhc-secure-dhcpv6] or authentication of DHCPv6 messages [RFC3315] are recommended.

The security updates will need to be made in two stages (immediately before and immediately after the event).

[Editor note: this section needs further work.]

## 7. IANA Considerations

This draft does not request any IANA action.

## 8. Acknowledgements

This work is illumined by RFC5887, so thank for RFC 5887 authors, Randall Atkinson and Hannu Flinck. Useful ideas were also illumined by documents from Tim Chown and Fred Baker. The authors also want to thank Wesley George, Olivier Bonaventure and other 6renum members for valuable comments.

## 9. Change Log [RFC Editor please remove]

draft-jiang-6renum-enterprise-00, original version, 2011-07-01

## 10. References

### 10.1. Normative References

- [RFC2608] Guttman, E., Perkins, C., Veizades, J., and M. Day "Service Location Protocol, Version 2", RFC 2608, June 1999.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.
- [RFC3633] Troan, O., and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.
- [RFC3646] R. Droms, "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.
- [RFC3956] Savola, P., and B. Haberman, "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address", RFC 3956, November 2004.
- [RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander "Secure Neighbor Discovery (SEND)", RFC 3971, March 2005.
- [RFC4193] Hinden, R., and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.
- [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.
- [RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.
- [RFC6106] Jeong, J., Ed., Park, S., Beloeil, L., and S. Madanapalli "IPv6 Router Advertisement Option for DNS Configuration", RFC 6106, November 2011.

## 10.2. Informative References

- [RFC2071] Ferguson, P., and H. Berkowitz., "Network Renumbering Overview: Why would I want it and what is it anyway?", RFC 2071, January 1997.
- [RFC2874] Crawford, M., and C. Huitema, "DNS Extensions to Support IPv6 Address Aggregation and Renumbering", RFC 2874, July 2000.
- [RFC3364] R. Austein, "Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6)", RFC 3364, August 2002.
- [RFC4192] Baker, F., Lear, E., and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", RFC 4192, September 2005.
- [RFC5887] Carpenter, B., Atkinson, R., and H. Flinck, "Renumbering Still Needs Work", RFC 5887, May 2010.
- [I-D.ietf-dhc-secure-dhcpv6]  
Jiang, S., and S. Shen, "Secure DHCPv6 Using CGAs", working in progress.
- [I-D.ietf-dhc-host-gen-id]  
S. Jiang, F. Xia, and B. Sarikaya, "Prefix Assignment in DHCPv6", draft-ietf-dhc-host-gen-id (work in progress), April, 2011.
- [I-D.liu-6renum-gap-analysis]  
Liu, B., and S. Jiang, "IPv6 Site Renumbering Gap Analysis", working in progress.

Author's Addresses

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

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

Brian Carpenter  
Department of Computer Science  
University of Auckland  
PB 92019  
Auckland, 1142  
New Zealand  
EMail: brian.e.carpenter@gmail.com

Network Working Group  
Internet Draft  
Intended status: Informational  
Expires: January 11, 2012

B. Liu  
S. Jiang  
Huawei Technologies Co., Ltd  
July 11, 2011

IPv6 Site Renumbering Gap Analysis  
draft-liu-6renum-gap-analysis-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 January 04, 2012.

Copyright 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

This document briefly introduces the existing mechanisms could be utilized by IPv6 site renumbering and envisions the effort could be done. This document tries to cover the most explicit issues and requirements of IPv6 renumbering. Through the gap analysis, the document provides a basis for future work to identify and develop



solutions or to stimulate such development as appropriate. The gap analysis is presented following a renumbering event procedure clue.

## Table of Contents

1. Introduction .....	3
2. Overall Requirements for Renumbering .....	3
3. Existing Components for IPv6 Renumbering .....	4
3.1. Relevant Protocols and Mechanisms .....	4
3.2. Management Tools .....	4
3.3. Procedures/Policies .....	5
4. Managing Prefixes .....	5
4.1. Prefix Delegation .....	5
4.2. Prefix Assignment .....	5
5. Address Configuration .....	6
5.1. Host Address Configuration .....	6
5.2. Router Address Configuration .....	7
5.3. Static Address Configuration .....	8
6. Address Relevant Entries Update .....	9
6.1. DNS Records Update .....	9
6.2. In-host Server Address Update .....	10
6.3. Filters .....	10
7. Renumbering Event Management .....	11
7.1. Renumbering Notification .....	11
7.2. Synchronization Management .....	12
7.3. Renumbering Monitoring.....	12
8. Miscellaneous .....	12
8.1. Multicast .....	12
8.2. Mobility .....	13
9. Gap Summary .....	13
9.1. Managing Prefixes .....	13
9.2. Address configuration .....	13
9.3. Address relevant entries update .....	14
9.4. Renumbering event management .....	15
10. Security Considerations .....	15
11. IANA Considerations .....	16
12. References .....	16
12.1. Normative References .....	16
12.2. Informative References .....	17
13. Acknowledgments .....	17

## 1. Introduction

As introduced in [RFC5887], renumbering, especially for medium to large sites and networks, is currently viewed as an expensive, painful, and error-prone process, avoided by network managers as much as possible. If IPv6 site renumbering continues to be considered difficult, network managers will turn to Provider Independent (PI) addressing for IPv6 to attempt to minimize the need for future renumbering. However, widespread use of PI may create very serious BGP4 scaling problems. It is thus desirable to develop tools and practices that may make renumbering a simpler process to reduce demand for IPv6 PI space.

This document performs a gap analysis to provide a basis for future work to identify and develop solutions or to stimulate such development as appropriate. Gap analysis draws on existing work in (at least) [RFC5887] and [RFC4192]. The [I-D.jiang-6renum-enterprise] contributions are incorporated into the more detailed gap analysis. In this document, we discuss the overall requirements for renumbering. The gap analysis is organized by the main steps of renumbering process, which include the prefix management, the node address (re)configuration, and address relevant entries update in various gateways, routers and servers, etc. Besides the steps, a sub-clause of renumbering event management is presented independently, which targets to help the operational/administrative process.

## 2. Overall Requirements for Renumbering

This section introduces the overall ultimate goals we want to achieve in renumbering event. Some existing mechanisms have already provide useful help. Further efforts may be achieved in the future.

- o Prefix delegation and delivery should be automatic and accurate in aggregation and coordination.
- o Address reconfiguration should be automatically achieved through standard protocols with minimum human intervene.
- o Address relevant entries update should be processed integrally and error-prevented. [Open Question]Is it necessary to develop automatic entries update mechanisms? If necessary, do we need standard protocols/interface for it?

- o [Open Question] Is it necessary/possible to develop a ''One-Click'' fully automatic renumbering technology? What scenarios have the potential possibility?
- o [Open Question] Is session survivability within our scope?

### 3. Existing Components for IPv6 Renumbering

#### 3.1. Relevant Protocols and Mechanisms

Generally, renumbering is achieved by utilizing existing protocols rather than dedicated renumbering protocols.

- o RA messages, defined in [RFC4861], are used to deprecate/announce old/new prefixes and to advertise the availability of an upstream router. In renumbering, it is one of basic mechanisms for host configuration.
- o When a host is renumbered, it may use SLAAC [RFC4862] for address configuration with the new prefix. Hosts receive RA messages which contain routable prefix(es) and the address(es) of the default router(s), then hosts can generate IPv6 address(es) by themselves.
- o Hosts configured through DHCPv6 [RFC3315] can reconfigure addresses by initialing RENEW sessions when the current addresses' lease time are expired or they receive the reconfiguration messages initiated by the DHCPv6 servers.
- o DHCPv6-PD (Prefix Delegation) [RFC3633] enables automated delegation of IPv6 prefixes using the DHCPv6. initiated
- o [RFC2894] defined standard ICMPv6 messages for router renumbering. This is a dedicated protocol for renumbering, but has not been widely used.

#### 3.2. Management Tools

Some operations of renumbering could be automatically processed by management tools in order to make the renumbering process more efficient and accurate. The tools may be designed dedicated for renumbering or just common tools could be utilized for some operations in renumbering.

Following are samples of the tools.

- o [LEROY] proposed a mechanism of macros to automatically update the address relevant entries/configurations inside the DNS, firewall, etc. The macros can be delivered through SOAP protocol from a network management server to the managed devices.
- o Asset management tools/systems. These tools may provide the ability of managing configuration files in nodes so that it is convenient to update the address relevant configuration in these nodes.

### 3.3. Procedures/Policies

- o [RFC4192] proposed a procedure for renumbering an IPv6 network without a flag day. The document includes a set of operational suggestions which can be followed step by step by network administrators.
- o [I-D.jiang-6renum-enterprise] analyzes the enterprise renumbering events and gives the recommendations among the existing renumbering mechanisms. According to the different stages, renumbering considerations are described in three categories: considerations and recommendations during network design, for preparation of enterprise network renumbering, and during renumbering operation

## 4. Managing Prefixes

When renumbering an enterprise site, a short prefix may be divided into longer prefixes for subnets. So we need to carefully manage the prefixes for prefix delivery, delegation, aggregation, synchronization, coordination, etc.

### 4.1. Prefix Delegation

Usually, the short prefix comes down from the operator and received by DHCPv6 server or router inside the enterprise network. The short prefix could be automatically delegated through DHCPv6-PD. Then the downlink DHCP servers or routers can begin advertising the longer prefixes to the subnets.

### 4.2. Prefix Assignment

When subnet routers receive the longer prefixes, they can directly assign them to the hosts. The prefix assignment overlaps with the host address configuration, which is described in the following section 5.1.

## 5. Address Configuration

### 5.1. Host Address Configuration

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 (It should be noted that, the prefix delivery could be achieved through DHCP according to the new IETF DHC WG document [I.D ietf-dhc-host-gen-id]). The DHCPv6-configured hosts can reconfigure addresses by initiating RENEW sessions when the current addresses' lease time are expired or receiving the reconfiguration messages initiated by the DHCPv6 servers.

#### o SLAAC and DHCPv6 address configuration co-existence

While an IPv6 site is being renumbered, both DHCPv6 and ND may be used to reconfigure the host addresses. The co-existence issue mainly includes following aspects:

##### - Dynamic upstream learning

[RFC5887] mentioned that, DHCP-configured hosts may want to learn about the upstream availability of new prefixes or loss of prior prefixes dynamically by deducing from periodic RA messages. But there is no standard 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.

##### - DHCP/SLAAC conflict

If the DHCP-managed 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 DHCP-v6 reconfiguration messages and finds the prefixes in the two protocols are different. This means serious network configuration error occurring.

[Open Question]It is hard for the host to identify the RA messages containing new prefix(es) representing adding an uplink or conflict caused by network configuration mistake.

- SLAAC-configured hosts finding DHCPv6 in use

[RFC5887] 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 multiple uplinks are available or 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.

- o DHCPv6 reconfigure bulk usage

[RFC5887] mentioned that "DHCPv6 reconfiguration doesn't appear to be widely used for bulk renumbering purposes".  
[Open Question] Using DHCPv6 reconfiguration can be considered as "stateful" renumbering which need sessions maintained between DHCP servers and clients. So maybe it is too heavy for the servers. So is it possible for bulk renumbering? Is there any requirement?

- o RA prefix lifetime limitation

In section 5.5.3 of [RFC4862], it is defined that "If the received Valid Lifetime is greater than 2 hours or greater than RemainingLifetime, set the valid lifetime of the corresponding address to the advertised Valid Lifetime." So when renumbering, if the previous RemainingLifetime is longer than two hours, it is impossible to reduce a prefix's lifetime less than two hours. This limitation is to prevent denial-of-service attack.  
[Open Question] This limitation requires renumbering to be planned in advance so that an immediate renumbering event is impossible. Should it be considered as a standard gap for renumbering?

## 5.2. Router Address Configuration

- o Learning new prefixes

As described in [RFC5887], "if a site wanted to be multihomed using multiple provider-aggregated (PA) routing prefixes with one prefix per upstream provider, then the interior routers would need a mechanism to learn which upstream providers and prefixes were currently reachable (and valid). In this case, their Router Advertisement messages could be updated dynamically to only advertise currently valid routing prefixes to hosts. This would be significantly more complicated if the various provider prefixes were of different lengths or if the site had non-uniform subnet prefix lengths."

- o Restart after renumbering

"Some routers cache IP addresses in some situations. So routers might need to be restarted as a result of site renumbering" [RFC2072].

After investigation, it seems (need further confirmation) this caused by individual implementation and only happen on the old type of routers. Therefore, it is not an issue anymore.

- o Router naming

In [RFC4192], it is suggested that "To better support renumbering, switches and routers should use domain names for configuration wherever appropriate, and they should resolve those names using the DNS when the lifetime on the name expires."

As [RFC5887] described, this capability is not new, and at least it is present in most IPsec VPN implementations. But many administrators do not realize that it could be utilized to avoid manual modification during renumbering.

[Open Question]Whether it is not easy to use or just suitable in few situations needs further investigation.

### 5.3. Static Address Configuration

Further gap analysis about static address issue could consider the following suggestions (proposed by George Wesley in the mail list).

- o Documenting how to limit the places where static addresses must be used (vs FQDN or autoconf).
- o Identifying gaps and proposing solutions in other areas to reduce the number of places that static addresses are required.

- o Documenting any gaps in [RFC4192] to make renumbering easier for a statically-numbered set of hosts and potentially identifying a problem statement for improving renumbering for static.

[Open Question] Besides the open questions above, the ULA utilization issue may also need consideration.

## 6. Address Relevant Entries Update

When nodes in a site have been renumbered, then all the entries in the site which contain the nodes' addresses must be updated. The entries mainly include DNS records and filters in various entities such as ACLs in firewalls/gateways.

### 6.1. DNS Records Update

- o DNS update automation

For DNS records update, most sites will achieve it by maintaining a DNS zone file and loading this file into the site's DNS server(s). Synchronization between host renumbering and the updating of its A6 or AAAA record is hard. [RFC5887] mentioned that an alternative is to use Secure Dynamic DNS Update [RFC3007], in which a host informs its own DNS server when it receives a new address. But Secure Dynamic DNS Update hasn't been widely deployed.

[Open Question] To popularize the [RFC3007] or to develop a lightweight dedicated protocol for this need to be considered.

DNS entries commonly have matching Reverse DNS entries which will also need to be updated during renumbering.

[Open Question] So synchronizing the procedures of forward and reverse DNS or even combining forward and reverse DNS updates in a single procedure also need to be considered.

- o DNS data structure optimization

[RFC2874] proposed a new A6 record type for DNS recording IPv6 address/prefix. And several extensions on query and processing were also proposed. With the A6 record and the extensions, an IPv6 address can be defined by using multiple DNS records. This feature increases the complexity of resolver but reduce the cost of zone file maintenance. So renumbering could be easier than AAAA record. But the [RFC2874] has not been widely used.



[Open Question]Is the DNS data structure optimization such as [RFC2874] necessary for easing renumbering? If necessary, is the optimization in [RFC2874] enough?

- o DNS authority

As described in [I-D.chown-v6ops-renumber-thinkabout], "it is often the case in enterprises that host web servers and application servers on behalf of collaborators and customers that DNS zones out of the administrative control of the host maintain resource records concerning addresses for nodes out of their control. When the service host renumbers, they do not have sufficient authority to change the records."

[Open Question]Whether it is only an operational issue or additional protocol/mechanism is needed to standardize the interaction between DNS systems needs to be considered.

## 6.2. In-host Server Address Update

While DNS records addresses of hosts in servers, hosts also record addresses of servers such as DNS server, radius server, etc. While renumbering, the hosts must update the records if the server addresses changed. Addresses of DHCPv6 servers do not need to be updated. They are dynamic discovered using DHCPv6 relevant multicast addresses.

- o The DNS server addresses for hosts are configured by DHCPv6. But current DHCPv6 messages do not indicate hosts the lifetimes of DNS. If the DNS lifetime expired and has been renumbered, the hosts may still use the old addresses. DHCPv6 should be extended to indicate hosts the associated DNS lifetimes when making DNS configuration. How does the DHCP server could know about the DNS lifetime is another issue.

## 6.3. Filters

- o Filters Management

Filters based on addresses or prefixes are usually spread in various devices. As [RFC5887] described, some address configuration data might be widely dispersed and much harder to find, even will inevitably be found only after the renumbering event. So there's a big gap for filter management.

In [LEROY], a server is used for managing filter update in various devices. But identifying where and which of the filters need to be updated during renumbering is still a gap.

- o Filter Update Automation Operation

As mentioned in section 3.2, [LEROY] proposed a mechanism which can automatically update the filters. The mechanism utilizes macros suitable for various devices such as routers, firewalls etc. to update the filter entries based on the new prefix. Such automation tool is valuable for renumbering because it can reduce manual operation which is error-prone and inefficiency.

[Open Question] Besides the macros, [LEROY] also proposed to use SOAP to deliver the macros to the devices. So there may be requirement of protocol standardization. [LEROY] uses application layer protocol while we may consider whether it is possible and suitable to use network layer protocol.

[Open Question] Update of filters based on prefixes and filters based on addresses may have different requirements and methods. For example, the prefix-based filters may consider to be updated through DHCPv6 server, which may provide better efficient.

## 7. Renumbering Event Management

From the perspective of network management, renumbering is a kind of event which may need additional process to make the process more easy and manageable.

### 7.1. Renumbering Notification

If hosts or servers are aware of a renumbering event happening, it may help the relevant process. Following are several examples of such additional process may ease the renumbering. Further contributions are expected.

- o A notification mechanism may be needed to indicate the hosts that a renumbering event of local recursive DNS happen or is going to take place.
- o [RFC4192] suggests that "reducing the delay in the transition to new IPv6 addresses applies when the DNS service can be given prior notice about a renumbering event." Reducing delay could improve the efficiency of renumbering.

## 7.2. Synchronization Management

### o DNS update synchronization

DNS update synchronization focuses on the coordinating between DNS and other entities/mechanisms, for example, as described in [RFC5887], synchronizing the SLAAC and DNS updates, and of reducing the SLAAC lease time and DNS TTL.

[Gaps TBD]

## 7.3. Renumbering Monitoring

While treating renumbering a network event, mechanisms to monitor the renumbering process may be needed. Considering the address configuration operation may be stateless(if ND is used for renumbering), it is difficult for monitoring. But for the DNS and filter update, it is quite possible to monitor the whole process.

[Gaps TBD]

## 8. Miscellaneous

### 8.1. Multicast

- o The embedding of IPv6 unicast addresses into multicast addresses and the embedded-RP (Rendezvous Point)[RFC3956] will cause issues when renumbering.

As [I-D.chown-v6ops-renumber-thinkabout] described, "If the RP address changes, then the group addresses must also be changed. This may happen not only when a site is renumbered, but also if a site is restructured or the RP is moved within the site. The embedded address is used by routers to determine the RP address. Applications must use new group addresses once the RP is not available on the old address."

- o Changing the unicast source address of a multicast sender might also be an issue for receivers.

As [I-D.chown-v6ops-renumber-thinkabout] described, "If a site's unicast prefix changes, then one will also need to change the multicast addresses. By way of example, a site renumbering away from prefix 2001:DB8:BEEF::/48" might have globally-scoped multicast addresses in use under the prefix "FF3E:30:2001:DB8:BEEF::/96". One may continue using the old addresses for a while, but this should be avoided since another

site may inherit the prefix and they may end up using the same multicast addresses.''

## 8.2. Mobility

- o [RFC5887] suggested that, for Mobile IP, define a better mechanism to handle change of home agent address while mobile is disconnected.

## 9. Gap Summary

### 9.1. Managing Prefixes

None. (call for contributions)

### 9.2. Address configuration

- o Host address configuration
  - SLAAC and DHCPv6 address configuration co-existence
    - Dynamic upstream learning:  
DHCP-configured host may want to learn about the upstream availability of new prefixes or loss of prior prefixes dynamically by deducing from periodic RA messages.
    - DHCP/SLAAC conflict:  
Prefixes in the two protocols' messages may be different, which may be caused by serious network configuration error. A diagnosis/report mechanism is needed here.
    - SLAAC-configured hosts find DHCPv6 is in use:  
RA messages contain 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.
  - DHCPv6 reconfigure bulk usage

Maybe it is too heavy for the server. So is it possible for bulk renumbering? Is there any requirement?
  - RA prefix lifetime limitation

If previous RemainingLifetime is longer than two hours, it is impossible to reduce a prefix's lifetime less than two hours. Is it a standard gap for renumbering?

- o Router address configuration

- Learning new prefixes

- If the site is multihoming, the interior routers would need a mechanism to learn which upstream providers and prefixes were currently reachable (and valid).

- Restart after renumbering

- Some routers cache IP addresses in some situations. So routers might need to be restarted as a result of site renumbering.

- Router naming

- Using domain names for routers is suitable in some scenarios but has not been widely deployed. Whether it is not easy to use or just suitable in few situations needs further investigation.

- o Static address configuration

Further work is needed.

### 9.3. Address relevant entries update

- o DNS records update

- DNS update automation

- Synchronization between host renumbering and the updating of its DNS records is hard. Forward and reverse DNS entries update may need to be combined together.

- DNS data structure optimization

- Is the DNS data structure optimization as A6 record [RFC2874] necessary for easing renumbering?

- DNS authority

- DNS zones are out of the administrative control. Authority collaboration is needed.

- o In-host server address update

Hosts also record addresses of servers such as DNS server addresses, radius server address, etc. While renumbering, the host must update the records if these server addresses changed.

- o Filters

- Filters management

- There is a gap of filter management to identify where and which of the filters need to be updated during renumbering. Manageable filter update may be also needed.

- Filter update automation operation

- Automation update tool is valuable for renumbering, and there may be requirement of protocol standardization to deliver of facility the tools.

#### 9.4. Renumbering event management

- o Renumbering notification

If hosts/servers are aware of a renumbering event happening, it may help the relevant process. A basic way is to extend current protocol messages to carry the renumbering notification.

- o Synchronization management

- DNS update synchronization

- An example is synchronizing the SLAAC and DNS updates, and of reducing the SLAAC lease time and DNS TTL.

- [TBD]

- o Renumbering monitoring

Mechanisms to monitor the process and feedback of renumbering may be needed. [TBD]

#### 10. Security Considerations

- o Prefix Validation

Prefixes from the ISP may need authentication to prevent prefix fraud. Announcing changes of site prefix to other sites (for example,

those that configure routers or VPNs to point to the site in question) also need validation.

In the LAN, Secure DHCPv6 ([I-D.ietf-dhc-secure-dhcpv6]) or SeND ([RFC3971], Secure Neighbor Discovery) deployment may need to validate prefixes.

- o Influence to Security Controls

During renumbering, security controls (e.g. ACLs) blocking access to legitimate resources should not be interrupted.

## 11. IANA Considerations

None.

## 12. References

### 12.1. Normative References

- [RFC2894] M. Crawford, "Router Renumbering for IPv6", RFC 2894, August 2000.
- [RFC2874] Crawford, M., and C. Huitema, "DNS Extensions to Support IPv6 Address Aggregation and Renumbering", RFC 2874, July 2000.
- [RFC3007] B. Wellington, "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.
- [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.
- [RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.
- [RFC3956] P. Savola, and B. Haberman. "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address.", RFC 3956, November 2004.
- [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.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

## 12.2. Informative References

- [RFC2072] H. Berkowitz, "Router Renumbering Guide" RFC2072
- [RFC4192] Baker, F., Lear, E., and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", RFC 4192, September 2005.
- [RFC5887] Carpenter, B., Atkinson, R., and H. Flinck, "Renumbering Still Needs Work", RFC 5887, May 2010.
- [I-D.ietf-dhc-secure-dhcpv6]  
Jiang, S., and Shen S., "Secure DHCPv6 Using CGAs", working in progress.
- [I-D.chown-v6ops-renumber-thinkabout]  
Chown, T., "Things to think about when Renumbering an IPv6 network", Work in Progress, September 2006.
- [I-D.jiang-6renum-enterprise]  
Jiang, S., and Liu B., " IPv6 Enterprise Network Renumbering Scenarios and Guidelines ", Working in Progress, July 2011.
- [LEROY] Leroy, D. and O. Bonaventure, "Preparing network configurations for IPv6 renumbering", International of Network Management, 2009, <<http://inl.info.ucl.ac.be/system/files/dleroy-nem-2009.pdf>>

## 13. Acknowledgments

This work adopts significant amounts of content from [RFC5887] and [I-D.chown-v6ops-renumber-thinkabout], so thank for Brian Carpenter, Randall Atkinson, Hannu Flinck, Tim Chown, Mark Thompson, Alan Ford, and Stig Venaas. Some useful materials were provided by Oliver Bonaventure and his student Damien Leroy, thanks for them, too.

Useful comments and contributions were made by George Wesley, and others.



This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Bing Liu  
Huawei Technologies Co., Ltd  
Huawei Building, No.3 Xinxu Rd.,  
Shang-Di Information Industry Base, Hai-Dian District, Beijing  
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  
P.R. China

Email: jiangsheng@huawei.com

