

Network Working Group
Internet Draft

Intended status: Best Current Practice
Expires: August 5, 2011

S. Jiang
B. Liu
Huawei Technologies Co., Ltd
January 26, 2011

IPv6 Site Renumbering Guidelines and Further Works
draft-jiang-ipv6-site-renum-guideline-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 August 5, 2011.

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 existing issues for IPv6 site renumbering. It also analyzes the possible directions to solve these issues and gives recommendations. This document only takes the perspective of network and network protocols. Renumbering in IPv4 networks, in the

Internet-Draftdraft-jiang-ipv6-site-renum-guideline-00.txt January 2011

dual-stack network or in the IPv4/IPv6 transition networks are out of scope.

This document only takes the perspective of network and network protocols. According to the different stages, these issues are described in three categories: considerations during network design, considerations for routine network management, and considerations during renumbering operation. Recommended solutions or strategies are also described. Issues that still remain unsolvable are listed as the fourth category.

Although we list a few non-network issues in this document, we consider them as issues that ISPs or network providers cannot affect. So, these issues are considered to be unsolvable and not explore further in these document, though they may be solved by OS implementations or application implementations.

We summary the requests that need to extend current protocols as further works at the end of this document.

Table of Contents

1.	Introduction	3
2.	Network Renumbering Considerations and Solutions/Strategies...	3
2.1.	Considerations/issues during network design	4
2.2.	Considerations/issues for the routine network management.	5
2.3.	Considerations/issues during renumbering operation.....	6
2.4.	Issues that still remain unsolvable	8
2.5.	Issues that need further analysis	9
3.	Non-network issues	9
4.	Requests to extend current protocol	10
5.	Security Considerations	11
6.	IANA Considerations	11
7.	Acknowledgements	11
8.	Change Log [RFC Editor please remove]	11
9.	References	11
9.1.	Normative References	11
9.2.	Informative References	12
	Author's Addresses	13

Internet-Draftdraft-jiang-ipv6-site-renum-guideline-00.txt January 2011

1. Introduction

[RFC5887] has reviewed the existing mechanisms for site renumbering for both IPv4 and IPv6, and identified operational issues with those mechanisms. However, the discussion and analysis were too wide. It exposure many issues, but not give enough analysis on whether these issues are solvable and how. Even the document itself indicates more fractionized and detailed analysis is needed. On another side, the mechanisms analyzed in the document are still not in used.

This document focuses on IPv6 network renumbering only, by leaving IPv4 out of scope. Renumbering in IPv4 networks, in the dual-stack network or in the IPv4/IPv6 transition networks are out of scope. This is also consistent preference from IETF renumber mail list by the time of writing up.

This document is mainly concerned with issues affecting medium to large sites, which is taken as the conclusion from [[RFC5887](#)]. It takes the analysis conclusions from [[RFC5887](#)] and other relevant documents as the primary input.

This document only takes the perspective of network and network protocols. According to the different stages, these issues are described in three categories: considerations during network design, considerations for routine network management, and considerations during renumbering operation. Recommended solutions or strategies are also described. Issues that still remain unsolvable are listed as the fourth category.

Issues that need further analysis are temporarily listed for now. They should all be relocated into abovementioned four categories.

Although we list a few non-network issues in this document, we consider them as issues that ISPs or network providers cannot affect. So, these issues are considered to be unsolvable and not explore further in these document, though they may be solved by OS

implementations or application implementations.

At the end of this document, we summary the requests that need to extend current protocols.

[2.](#) Network Renumbering Considerations and Solutions/Strategies

The purpose of this section is not to describe the renumbering operation or event completely or entirely, but to expose the existing issues and give the recommended solutions or strategies.

Jiang & Liu

Expires August 5, 2011

[Page 3]

Internet-Draftdraft-jiang-ipv6-site-renum-guideline-00.txt January 2011

[2.1.](#) Considerations/issues 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.

- 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](#)]). (Manual address configuration is not scalable in medium to large sites, hence be out of scope.)

SLAAC is considered easier to renumbering 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 large number of interactions between hosts and DHCPv6 server. However, DHCPv6 reconfiguration "doesn't appear to be widely used for bulk renumbering purposes" [[RFC5887](#)].

In principle, a network should choice only one address configuration model and employs either ND or DHCPv6. 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 subnets may reduce the risk partly.

On another side, new protocol extension may help to diagnose the fault situation. This diagnose function could be particularly useful in the scenario where a multihomed network uses SLAAC for one address prefix and DHCPv6 for another.

- 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. Manually on-demand updating

Internet-Draft draft-jiang-ipv6-site-renom-guideline-00.txt January 2011

model is considered as a harmful problem creator in renumbering event.

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 Neighbour 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

Addresses should not be used to configure network connectivity, such as tunnels. 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.

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

[2.2.](#) Considerations/issues for the routine network management

This session describes several recommendations for the routine network management. To adopt these recommendations, a site could be renumbered easier. However, these recommendations are not cost free. They are possible to increase the daily burden of networks. Therefore, only these networks that are expected to be renumbered soon or very frequent 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.

- Reduce the NAT mapping session keepalive time.

Idle NAT mapping session may be keep alive for a long period if the external network addresses space is plenteous and the internal network address architecture is stable. However, renumbering events mean to restructure the internal network address architecture fully or partly. Reducing the NAT mapping session keepalive time may help to tear down the idle TCP connectivities. This will reduce the TCP surviving issue during the renumbering event.

2.3. Considerations/issues 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.

- Transition period

If renumbering transition period is longer than all addresses life, 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.

- 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 happen or is going to take place.

- Router awareness

In a site with multiple border routers, portion renumbering should be aware by all border routers 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.

- NAT or tunnel concentrator renumbering

NAT or tunnel concentrator itself might be renumbered. This change should be reconfigured to relevant hosts or router.

[2.4.](#) Issues that still remain unsolvable

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

- 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.
- 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) 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 NAT or 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.

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

[2.5.](#) Issues that need further analysis

This section lists a few issues that still need further analysis. Some of them may be addressed in later version of this document and relocated into other sections. Some of them may be worthy separated document. (Editor note: if all issues addressed, this section should be removed.)

- "Some routers cache IP addresses in some situations. So routers might need to be restarted as a result of site renumbering" [[RFC2072](#)]. It seems this caused by individual implementation and only happen on the old type of routers. (Author note: to be removed, if confirmed)
- Multihomed site, using SLAAC for one address prefix and DHCPv6 for another, would clearly create a risk of inconsistent host behaviour and operational confusion.
- It seems so far the renumbering studies only focusing on the individual network using a single prefix. In a large network, a short prefix may be used. The prefix is assigned to be longer and prefixes and delegated to several sub-networks. To make the scenario even more complicated, it may be some sub-networks employ SLAAS while some others are managed by DHCPv6. How to coordinate among these sub-networks to be renumbered together may be worth of analyzing.
- The impact of portion renumbering may need to be analyzed further.

[3.](#) Non-network issues

Although we focus on network side, in this section, we also list a few non-network issues. They are out of network providers/operators reach. Therefore, from network perspective, these issues are considered to be unsolvable though they may be solved by OS implementations or application/service implementations. It is out of scope to explore these issues further.

- Any implementation is at risk from renumbering if it does not check that an address is valid each time it opens a new communications session
- Socket API encourages applications to be aware of and to store IP address. And the API relative functions do not return an address lifetime so that applications have no way to know the address is no longer valid.

- "DNS Pining": limits acceptance of server IP address changes for JavaScript security considerations and it may directly

damage the ability of applications to deal with renumbering.

- Server applications might need to be restarted when the host they contain is renumbered. In an IPv6 multi-addressed host, server applications need to be able to listen on more than one address simultaneously. Name-based APIs or implementations are recommended.
- When a nameserver is renumbered, the host may not be aware or notified immediately; or even the host is notified, but it still considers the old nameserver is available. The host will at some point find it unavailable. This will cause name resolving failure though these failure may be recoverable.
- Renumbering may cause issues for ACLs or group login services.

[4.](#) Requests to extend current protocol

As mentioned in [section 2](#), the following request to extend the current protocols.

- A diagnose function to detect and report the confliction of SLAAC and DHCPv6 address assignment.
- The current protocol needs to be extended if it does not support to combine the forward and reverse DNS updates in a single procedure. (Author note: it seems possible. If so, remove this item.)
- DHCPv6 should be extended to indicate hosts the associated DNS lifetimes when making DNS configuration.
- A lightweight renumbering specific security mechanism may be developed if SEND is too weight to be widely deployed.
- If the issues of coordination among these sub-networks to be renumbered together are confirmed, new interaction may need to be defined to achieve the cooperation.
- 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 recursive.

- NAT or tunnel concentrator configuration procedure may need to be extended to be able to notify the host the renumbering of NAT or tunnel concentrator.

5. 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.]

6. IANA Considerations

This draft does not request any IANA action.

7. Acknowledgements

This work is illumined by [RFC5887](#), so thank for [RFC 5887](#) authors, Brian Carpenter, Randall Atkinson and Hannu Flinck. Useful ideas were also illumined by documents from Tim Chown and Fred Bark.

8. Change Log [RFC Editor please remove]

[draft-jiang-ipv6-site-renumbering-ps-00](#), original version, 2011-01-28

9. References

9.1. 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.

Internet-Draftdraft-jiang-ipv6-site-renum-guideline-00.txt January 2011

- [RFC3646] R. Droms, "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6) ", [RFC3646](#), December 2003.
- [RFC3736] R. Droms, "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", [RFC 3736](#), April 2004.
- [RFC3971] J. Arkko, Ed., J. Kempf, B. Zill, 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.
- [RFC6106] J. Jeong, Ed., S. Park, L. Beloeil, and S. Madanapalli "IPv6 Router Advertisement Option for DNS Configuration", [RFC 6106](#), November 2011.

[9.2](#). Informative References

- [RFC4076] Chown, T., Venaas, S., and A. Vijayabhaskar, "Renumbering Requirements for Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 4076](#), May 2005.
- [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.

Internet-Draftdraft-jiang-ipv6-site-renum-guideline-00.txt January 2011

Author's Addresses

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: shengjiang@huawei.com

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

