Network Working Group
Internet Draft
Intended status: Informational
Expires: May 27, 2013

S. Jiang
B. Liu
Huawei Technologies Co., Ltd
B. Carpenter
University of Auckland

November 28, 2012

IPv6 Enterprise Network Renumbering Scenarios and Guidelines
draft-ietf-6renum-enterprise-04.txt

Status of this Memo

Copyright Notice

Abstract

This document analyzes events that cause renumbering and describes the best renumbering practice. Best practices are described in three categories: those applicable during network design, those applicable during preparation for renumbering, and those applicable during the renumbering operation.

Table of Contents

1. Introduction

Site renumbering is difficult. Network managers frequently attempt to avoid renumbering by numbering their network resources from Provider Independent (PI) address space. However, widespread use of PI might create serious BGP4 scaling problems and according to Regional Internet Registry (RIR) policies, PI space is not always available for enterprises Therefore, it is desirable to develop mechanisms that simplify IPv6 renumbering.

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

Since the IPv4 and IPv6 are logically separated from the perspective of renumbering, regardless of overlapping of the IPv4/IPv6 networks or devices, 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.

This document focuses on enterprise network renumbering, however, most of the analysis is also applicable to ISP network renumbering. Renumbering in home networks is out of scope, but it can also benefit from the analysis in this document.

The concept of enterprise network and a typical network illustration are introduced first. Then, best renumbering practices are introduced according to the following categories: those applicable during network design, those applicable during preparation for renumbering, and those applicable during the renumbering operation.

2. Enterprise Network Illustration for Renumbering

An Enterprise Network as defined in [RFC4057] is: a network that has multiple internal links, one or more router connections to one or more Providers, and is actively managed by a network operations entity.

Figure 1 provides a sample enterprise network architecture. Those entities relevant to renumbering are highlighted.

Address reconfiguration is fulfilled either by Dynamic Host configuration Protocol for IPv6 (DHCPv6) or Neighbor Discovery for IPv6 (ND) protocols. During the renumbering event, the Domain Name Service (DNS) records need to be synchronized while routing tables,

Access Control Lists (ACLs) and IP filtering tables in various devices also need to be updated, too.

Static address issue is described in a dedicated draft [I-D.ietf-6renum-static-problem].

```
            Uplink 1            Uplink 2
               |                   |
           +---+---+           +---+---+
     +---- |Gateway| --------- |Gateway| -----+
     |     +-------+           +-------+      |
     |          Enterprise Network            |
     |   +------+     +------+    +------+    |
     |   | APP  |     |DHCPv6|    |  DNS |    |
     |   |Server|     |Server|    +Server+    |
     |   +---+--+     +---+--+    +--+---+    |
     |       |            |          |        |
     |    ---+--+---------+------+---+-       |
     |          |                |            |
     |       +--+---+        +---+--+         |
     |       |Router|        |Router|         |
     |       +--+---+        +---+--+         |
     |          |                |            |
     |     -+---+----+-------+---+--+-        |
     |      |        |       |      |         |
     |    +-+--+  +--+-+  +--+-+  +-+--+      |
     |    |Host|  |Host|  |Host|  |Host|      |
     |    +----+  +----+  +----+  +----+      |
     +----------------------------------------+
```

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. IPv4/IPv6 co-existence 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 divide enterprise network renumbering scenarios into two categories defined by external and internal network factors, which require renumbering for different reasons.

3.1. Renumbering Caused by External Network Factors

The following ISP uplink-related events can cause renumbering:

- o The enterprise network switches to a new ISP. When this occurs, the enterprise stop numbering its resources form the prefix allocated by the old ISP and renumbers its resources from the prefix allocated by the new ISP.

  When the enterprise switches ISPs, a "flag day" renumbering event [RFC4192] may be averted if, during a transitional period, the enterprise network may number its resources from either prefix. One way to facilitate such a transitional period is for the enterprise to contract for service from both ISPs during the transition.

- o The renumbering event can be initiated by receiving new prefixes from the same uplink. This might happen if the enterprise network is 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. Alternatively, the ISP itself might be renumbered due to topology changes 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 purposes. This might not be a typical renumbering case because the original addresses will not be changed. However, initial numbering may be considered as a special renumbering event. The enterprise network removes uplink(s) or old prefixes.

3.2. Renumbering caused by Internal Network Factors

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

- o The enterprise network might proactively adopt a new address scheme, for example by switching to a new transition mechanism or stage of a transition plan.

- o The enterprise network might reorganize its topology or subnets.

4. Network Renumbering Considerations and Best Current Practices

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 recommends some solutions or strategies for the enterprise renumbering, chosen among existing mechanisms. There are known gaps analyzed by [I-D.ietf-6renum-gap-analysis]. If these gaps are filled in the future, the enterprise renumbering can be processed more automatically, with fewer issues.

4.1. Considerations and Best Current Practices during Network Design

This section describes the consideration or issues relevant to renumbering that a network architect should carefully plan when building or designing 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] and [RFC6603] provide a mechanism for automated delegation of IPv6 prefixes. Normally, DHCPv6 PD options are used between the internal enterprise routers, for example, a router receives prefix (es) from its upstream router (might be a border gateway or edge router .etc) through DHCPv6 PD options and then advertise it (them) to the local hosts through RA messages.

- Usage of FQDN

In general, Fully-Qualified Domain Names (FQDNs) are recommended to be used to configure network connectivity, such as tunnels, servers etc. 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.

Note that, using FQDN would rely on DNS systems. For a link local network that does not have a DNS system, multicast DNS [I-D.cheshire-dnsext-multicastdns] could be utilized. For some specific circumstances, using FQDN might not be proper if adding DNS service in the node/network would cause un-desired complexity or issues.

Service discovery protocols such as Service Location Protocol [RFC2608], multicast DNS with SRV records and DNS Service Discovery [I-D.cheshire-dnsext-dns-sd] can engage using FQDN and reduce the number of places that IP addresses need to be

configured. But it should be noted that these protocols are normally used link-local only.

- Usage of ULA

Unique Local Addresses (ULAs) are defined in [RFC4193] as provider-independent prefixes. And since there is a 40 bits pseudo random field in the ULA prefix, there is no practical risk of collision (please refer to section 3.2.3 in [RFC4193] for more detail). For enterprise networks, using ULA along with PA can provide a logically local routing plane separated from the globally routing plane. The benefit is to ensure stable and specific local communication regardless of the ISP uplink failure. This benefit is especially meaningful for renumbering. It mainly includes three use cases as the following.

During the transition period, it is desirable to isolate local communication changes in the global routing plane. If we use ULA for the local communication, this isolation is achieved.

Enterprise administrators might want to avoid the need to renumber their internal-only, private nodes when they have to renumber the PA addresses of the whole network because of changing ISPs, ISPs restructuring their address allocation, or any other reasons. In these situations, ULA is an effective tool for the internal-only nodes.

For multicast, ULA can be a way of avoiding renumbering from having an impact on multicast. In most deployments multicast is only used internally (intra-domain), and the addresses used for multicast sources and Rendezvous-Points need not be reachable nor routable externally. Hence one may at least internally make use of ULA for multicast specific infrastructure.

- Address Types

This document focuses on the dynamically-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 are out of scope. Manually-configured addresses/hosts should be avoided as much as possible.

- Address configuration models

In IPv6 networks, there are two auto-configuration models for address assignment: Stateless Address Auto-Configuration (SLAAC, [RFC4862]) by Neighbor Discovery (ND, [RFC4861]) and stateful address configuration by Dynamic Host Configuration Protocol for IPv6 (DHCPv6, [RFC3315]). In the latest work, DHCPv6 can also support host-generated address model by assigning a 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 might cause a large number of interactions between hosts and DHCPv6 server.

This document has no preference between ND and DHCPv6 address configuration models. It is network architects' job to decide which configuration model is employed. But it should be noticed that using DHCPv6 and ND together within one network, especially in one subnet, might cause operational issues. For example, some hosts use DHCPv6 as the default configuration model while some use ND. Then the hosts' address configuration model depends on the policies of operating systems and cannot be controlled by the network. Section 5.1 of [I-D.ietf-6renum-gap-analysis] discusses more details on this topic. So, in general, this document recommends using DHCPv6/SLAAC independently in different subnets.

However, since DHCPv6 is also used to configure many other network parameters, there are ND and DHCPv6 co-existence scenarios. Combinations of address configuration models might coexist within a single enterprise network. [I-D.ietf-savi-mix] provides recommendations to avoid collisions and to review collision handling in such scenarios.

- DNS

It is recommended that the site have an automatic and systematic procedure for updating/synchronizing its DNS records, including both forward and reverse mapping [RFC2874]. A manual on-demand updating model does not scale, and increases the chance of errors.

Although the A6 DNS record model [RFC2874] was designed for easier renumbering, it left many unsolved technical issues [RFC3364]. Therefore, it has been moved to historic status [RFC6563] and is not recommended.

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

Often, a small site depends on its ISP's DNS system rather than maintaining its own. When renumbering, this requires administrative coordination between the site and its ISP.

The DNS synchronization can be completed through the Secure DNS Dynamic Update [RFC3007]. Dynamic DNS update can be provided by the DHCPv6 client or by the server on behalf of individual hosts. [RFC4704] defined a DHCPv6 option to be used by DHCPv6 clients and servers to exchange information about the client's FQDN and about who has the responsibility for updating the DNS with the associated AAAA and PTR (Pointer Record) RRs (Resource Records). For example, if a client wants the server to update the FQDN-address mapping in the DNS server, it can include the Client FQDN option with proper settings in the SOLICIT with Rapid Commit, REQUEST, RENEW, and REBIND message originated by the client. When DHCPv6 server gets this option, it can use the dynamic DNS update on behalf of the client. In this document, we promote to support this FQDN option. But since it's a DHCPv6 option, it implies that only the DHCP-managed networks are suitable for this operation. In SLAAC mode, sometimes hosts also need to register addresses on a registration server, which could in fact be a DHCPv6 server (as described in [I-D.ietf-dhc-addr-registration]); then the server would update corresponding DNS records.

- Security

Any automatic renumbering scheme has a potential exposure to hijacking. Malicious entity in the network can forge prefixes to renumber the hosts. So proper network security mechanisms are needed.

For ND, Secure Neighbor Discovery (SEND, [RFC3971]) is a possible solution, but it is complex and there's almost no real deployment so far. Comparing the non-trivial deployment of SEND, RA guard [RFC6105] is a light-weight alternative, which focuses on rogue router advertisements proof in a L2 network. However, it also hasn't been widely deployed since it hasn't been published for long.

For DHCPv6, there are built-in secure mechanisms (like Secure DHCPv6 [I-D.ietf-dhc-secure-dhcpv6]), and authentication of DHCPv6 messages [RFC3315] could be utilized. But these security mechanisms also haven't been verified by wide real deployment.

- Miscellaneous

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

4.2. Considerations and Best Current Practices for the Preparation of Renumbering

In ND, 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 section describes several recommendations for the preparation of enterprise renumbering event. By adopting these recommendations, a site could be renumbered more easily. However, these recommendations might increase the daily traffic, server load, or burden of network operation. Therefore, only those networks that are expected to be renumbered soon or very frequently should adopt these recommendations, with balanced consideration between daily cost and renumbering cost.

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

Long-lifetime addresses might cause issues for renumbering events. Particularly, some offline hosts might reconnect using these addresses after renumbering events. Shorter preferred lifetimes with relatively long valid lifetimes may allow short transition periods for renumbering events and avoid frequent address renewals.

- Reduce the DNS record TTL on the local DNS server.

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

Recent research [BA2011] [JSBM2002] indicates that it is both practical and reasonable for A, AAAA, and PTR records that belong to leaf nodes of the DNS (i.e. not including the DNS root or DNS top-level domains) to be configured with very short DNS TTL values, not only during renumbering events, but also for longer-term operation.

- 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. In ND, The DNS configuration can be done through reducing the lifetime value in RDNSS option [RFC6106]. In DHCPv6, the DNS configuration option specified in [RFC3646] doesn't provide lifetime attribute, but we can reduce the DHCPv6 client lease time to achieve similar effect.

- Identify long-living sessions

Any applications which maintain very long transport connections (hours or days) should be identified in advance, if possible. Such applications will need special handling during renumbering, so it is important to know that they exist.

4.3. Considerations and Best Current Practices 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 unavailable for a period until the renumbering event is completed. It is efficient and provides convenience for network operation and management. But network outage is usually unacceptable for end users and enterprises. A renumbering procedure without a flag day provides smooth address switching, but much more operational complexity and difficulty is introduced.

- Transition period

If renumbering transition period is longer than all address lifetimes, after which the address leases expire, each host will automatically pick up its new IP address. In this case, it would be the DHCPv6 server or Router Advertisement itself that automatically accomplishes client renumbering.

Address deprecation should be associated with the deprecation of associated DNS records. The DNS records should be deprecated as early as possible, before the addresses themselves.

- Network initiative enforced renumbering

If the network has to enforce renumbering before address leases expire, the network should initiate DHCPv6 RECONFIGURE messages. For some operating systems such as Windows 7, if the hosts receive RA messages with ManagedFlag=0, they'll release the DHCPv6 addresses and do SLAAC according to the prefix information in the RA messages, so this could be another enforcement method for some specific scenarios.

- Impact to branch/main sites

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

- DNS record update and DNS configuration on hosts

DNS records on the local DNS server 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 TTLs of DNS records are shorter than the transition period, an administrative operation might 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 server addresses might co-exist on the hosts. If the lifetime of DNS configuration is shorter than the transition period, name resolving failure may be reduced to minimum.

- Tunnel concentrator renumbering

A tunnel concentrator itself might be renumbered. This change should be reconfigured in relevant hosts or routers, unless the configuration of tunnel concentrator was based on FQDN.

For IPSec, [RFC2230] defines the KX (Key eXchange) record, which could be used to help locate the domain-name for an IPsec VPN concentrator associated with a site's domain name. For current practice, the community needs to change its bad habit of using

IPsec in an address-oriented way, and renumbering is one of the main reasons for that.

- Connectivity session survivability

During the renumbering operations, connectivity sessions in IP layer would break if the old address is deprecated before the session ends. However, the upper layer sessions can survive by using session survivability technologies, such as SHIM6 [RFC5533]. As mentioned above, some long-living applications may need to be handled specially.

5. Security Considerations

As noted, a site that is listed by IP address in a black list can escape that list by renumbering itself.

Any automatic renumbering scheme has a potential exposure to hijacking. Proper network security mechanisms are needed. Although there are some existing security mechanisms such as SEND, RA guard, secure DHCPv6 etc., they haven't been widely deployed and haven't been verified whether they are not bringing too much operational complexity and cost.

Dynamic DNS update might bring risk of DoS attack to the DNS server. So along with the update authentication, session filtering/limitation might also be needed.

The "make-before-break" approach of [RFC4192] requires the routers keep advertising the old prefixes for some time. But if the ISP changes the prefixes very frequently, the co-existence of old and new prefixes might cause potential risk to the enterprise routing system since the old address relevant route path might already invalid and the routing system just doesn't know it. However, normally enterprise scenarios don't involve the extreme situation.

6. IANA Considerations

This draft does not request any IANA action.

7. Acknowledgements

This work is illuminated by RFC5887, so thank for RFC 5887 authors, Randall Atkinson and Hannu Flinck. Useful ideas were also presented in 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.

8. References

8.1. Normative References

[RFC2608] Guttman, E., Perkins, C., Veizades, J., and M. Day "Service Location Protocol, Version 2", RFC 2608, June 1999.

[RFC3007] B. Wellington, "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.

[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.

[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.

[RFC4704] B. Volz, "The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option", RFC 4706, October 2006.

[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.

8.2. Informative References

[RFC2230] R. Atkinson, "Key Exchange Delegation Record for the DNS", RFC 2230, November 1997.

[RFC2874] Crawford, M., and C. Huitema, "DNS Extensions to Support IPv6 Address Aggregation and Renumbering", RFC 2874, July 2000.

[RFC3363] R. Bush, A. Durand, B. Fink, O. Gudmundsson, T. Hain, "Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)", RFC 3363, August 2002.

[RFC3364] R. Austein, "Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6)", RFC 3364, August 2002.

[RFC4057] J. Bound, Ed. "IPv6 Enterprise Network Scenarios", RFC 4057, June 2005.

[RFC4192] Baker, F., Lear, E., and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", RFC 4192, September 2005.

[RFC5533] Nordmark, E., and Bagnulo, M., "Shim6: Level 3 Multihoming Shim Protocol for IPv6", RFC 5533, June 2009.

[RFC5887] Carpenter, B., Atkinson, R., and H. Flinck, "Renumbering Still Needs Work", RFC 5887, May 2010.

[RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105, February 2011.

[RFC6563] Jiang, S., Conrad, D. and Carpenter, B., "Moving A6 to Historic Status", RFC 6563, May 2012.

[RFC6603] J. Korhonen, T. Savolainen, S. Krishnan, O. Troan, "Prefix Exclude Option for DHCPv6-based Prefix Delegation", RFC 6603, May 2012.

[I-D.ietf-dhc-secure-dhcpv6]
Jiang, S., and S. Shen, "Secure DHCPv6 Using CGAs", working in progress, March 2012.

[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), August, 2012.

[I-D.ietf-savi-mix]
Bi, J., Yao, G., Halpern, J., and Levy-Abegnoli, E., "SAVI for Mixed Address Assignment Methods Scenario", working in progress, April 2012.

[I-D.ietf-dhc-addr-registration]
Jiang, S., Chen, G., "A Generic IPv6 Addresses Registration Solution Using DHCPv6", working in progress, May 2012.

[I-D.ietf-6renum-gap-analysis]
Liu, B., and Jiang, S., "IPv6 Site Renumbering Gap Analysis", working in progress, August 2012.

[I-D.ietf-6renum-static-problem]
Carpenter, B. and S. Jiang., "Problem Statement for Renumbering IPv6 Hosts with Static Addresses", working in progress, August 2012.

[I-D.cheshire-dnsext-dns-sd]
Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", draft-cheshire-dnsext-dns-sd-11 (work in progress), December 2011.

[I-D.cheshire-dnsext-multicastdns]
Cheshire, S. and M. Krochmal, "Multicast DNS", draft-cheshire-dnsext-multicastdns-15 (work in progress), December 2011.

[BA2011] Bhatti, S. and R. Atkinson, "Reducing DNS Caching", Proc. 14th IEEE Global Internet Symposium (GI2011), Shanghai, China. 15 April 2011.

[JSBM2002] J. Jung, E. Sit, H. Balakrishnan, & R. Morris, "DNS Performance and the Effectiveness of Caching", IEEE/ACM Transactions on Networking, 10(5):589-603, 2002.

Author's Addresses

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

EMail: jiangsheng@huawei.com

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

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland, 1142
New Zealand

EMail: brian.e.carpenter@gmail.com