IPv6 Site Renumbering Guidelines and Further Works

draft-jiang-ipv6-site-renum-guideline

IETF 80 RENUM BoF

March 31, 2010

Sheng Jiang(Speaker)

Bing Liu

Introduction

- **Renumbering is not new. We stand on the shoulders of giants**
- **RFC5887 "Renumbering Still Needs Work", by B. Carpenter**
  - RFC1900 "Renumbering Needs Work", by B. Carpenter
  - RFC4192, RFC4076, RFC2894, RFC2874, RFC2072, RFC2071, RFC1916
  - Credits to B. Carpenter, F. Baker, T. Chown, M. Crawford, R. Droms, etc.
- **Analyzes the existing issues for IPv6 site renumbering**
- **Analyzes the possible directions to solve these issues and gives recommendations**
  - Many issues can be avoided if networks are well-designed and well-managed
  - Some issues need to extra functions beyond the current protocols
  - Some issues may not solvable
- **Only takes the perspective of network and network protocols**
- **IPv6 only. Renumbering in IPv4 networks, in the dual-stack network or in the IPv4/IPv6 transition networks are out of scope**

Analysis structure

- **Issues are described in three categories with recommended solutions or strategies:**
  - considerations during network design
  - considerations for routine network management
  - considerations during renumbering operation
- **Issues that still remain unsolvable are listed as the fourth category**
- **A few non-network issues is also listed**
  - these issues are considered to be unsolvable from ISP perspective,
  - they may be solved by OS or application implementations
- **Summary the requests that need to extend current protocols as further works**

Considerations/issues during network design (1)

- **Address configuration models**
  - It is recommended that a network should choose only one host-oriented address configuration model, either SLAAC by ND or stateful address configuration by DHCPv6
  - ND and DHCPv6 co-existing is possible with many potential issues
    - draft-liu-ipv6-renum-conflicts proposes a diagnose and report mechanism
- **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

Considerations/issues during network design (2)

- **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
    - SEND [RFC3971] is recommended
    - Alternatively, certain lightweight renumbering specific security mechanism may be developed
- **Miscellaneous**
  - Addresses should not be used to configure network connectivity
    - Such as tunnel, addresses from other sites or networks, etc.
    - Fully-Qualified Domain Names should be used
    - Service Location Protocol and multicast DNS with SRV records for service discovery

Considerations/issues for the routine network management

Stable records or long lifetimes mean less flexibility

- **Reduce the address preferred time or valid time or both**
- **Reduce the DNS record TTL**
- **Reduce the DNS configuration lifetime on the hosts**
- **Reduce the NAT mapping session keepalive time**

- **These recommendations are 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**

Considerations/issues during renumbering operation (2)

- **Transition period**
  - If renumbering transition period is longer than all addresses lifetime, ND or DHCPv6 can 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
- **DNS record update and DNS configuration on hosts**
  - DNS records should be updated if hosts are renumbered. 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. 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

Considerations/issues during renumbering operation (2)

- **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, 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

Issues that still remain unsolvable (1)

- **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**

Issues that still remain unsolvable (2)

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

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

Issues that need further analysis

- **"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 split into several longer prefixes and delegated to several sub-networks. How to coordinate among these sub-networks to be renumbered together may be worth of analyzing. (To make the scenario even more complicated, it may be some sub-networks employ SLAAS while some others are managed by DHCPv6.)
- **The impact of portion renumbering may need to be analyzed further.**

Non-network issues

- **"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.**

Identified requests to extend 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**

- **Questions, clarifications?**

- **Thanks**