IPv6 Enterprise Network Renumbering Scenarios and Guidelines

draft-jiang-6renum-enterprise

IETF 82 RENUM WG

November 18, 2011

Sheng Jiang

Bing Liu

Brian Carpenter (Speaker)

Changes from v00 and WG choices

- **According to IETF 81 onsite discussions and mail list:**
  - Add several more renumbering reasons
  - We can not do much about manual configured hosts
  - Static addresses is separated into another document
  - ULA usage is out of scope – another document submitted to v6ops WG
  - ND and DHCPv6 co-existing references to mature document from SAVI WG
  - A6 is problematic, should be avoided though it was designed for renumbering purpose
  - Secure Dynamic DNS Update is recommended
    - DNS update may be made by DHCPv6 server rather than hosts

Structure of Draft

- Section 1: background and introduction
- Section 2: Enterprise Network introduction and illustration
- Section 3: Enterprise Network Renumbering Scenario Categories (According to different reasons)
- Section 4: According to the different stages of renumbering events, considerations and best current practise are described in three categories:
  - during network design
  - for preparation of renumbering
  - during renumbering operation
- Section 5: A gap inventory is listed at the end of this document
  - [Still Open Question] Should we summary here or leave all to gap analysis draft

Considerations and Best Current Practice during network design (1)

- **Prefix Delegation**
  - DHCPv6-PD provides an automatic delegation mechanism
    - Will Homenet provide additional solutions for enterprise use?
  - RFC3633 and draft-ietf-dhc-pd-exclude
- **Usage of FQDN**
  - FQDNs should be used to configure network connectivity, such as tunnels.
  - 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

Considerations and Best Current Practice during network design (2)

- **Address Types**
  - Focuses on the dynamic-configured global unicast addresses
  - Manual-configured addresses should be
  - Unique Local Address may be used on local routers or servers, which only intends for local communications.
- **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
    - draft-ietf-savi-mix provides recommendations to avoid collisions and to review collision handling in such scenarios.

Considerations and Best Current Practice during network design (3)

- **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
  - A manually on-demand updating model is considered as a harmful **source of problems** in renumbering event
  - A6 DNS is not recommended though it was designed for renumbering purpose
  - The Secure Dynamic DNS Update provides the capability of auto DNS synchronizing

Considerations and Best Current Practice during network design (4)

- **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 to replace ND
    - DHCPv6 build-in secure mechanisms, like Secure DHCPv6 or authentication of DHCPv6 messages, are recommended
- **Miscellaneous**
  - A site or network should also avoid to embedding addresses from other sites or networks in its own configuration data

Considerations and Best Current Practice 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.**
- **Stable records or long lifetimes mean less flexibility**
  - Reduce the address preferred time or valid time or both
  - Reduce the DNS record TTL on local DNS servers
  - Reduce the DNS configuration lifetime on the hosts
  - **Identify long-living sessions**
- **They might increase the burden of network operation. Therefore, only those networks that are expected to be renumbered soon or very frequently should adopt these recommendations**

Considerations and Best Current Practice during renumbering operation (1)

- **Within/without a flag day**
- **Transition period**
  - If renumbering transition period is longer than all address lifetimes, ND or DHCPv6 can automatically accomplishes client renumbering
  - **Address deprecation should be associated with the deprecation of associated DNS records**
- **Network initiative enforced renumbering**
  - If the network has to enforce renumbering before address leases expire, the network should initiate enforcement 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

Considerations and Best Current Practice during renumbering operation (2)

- **DNS record update and DNS configuration on hosts**
  - DNS records on the local DNS server 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.
    - 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 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

Considerations and Best Current Practice during renumbering operation (3)

- **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
- **Tunnel concentrator renumbering**
  - Tunnel concentrator itself might be renumbered. This change should be reconfigured to relevant hosts or router
- **Connectivity session survivability**

Comments are welcomed!

Adopt as WG document?

Agree to BCP as intended status?

Thank You!