IPv6 Site Renumbering Gap Analysis

draft-ietf-6renum-gap-analysis-01

Bing Liu(speaker), Sheng Jiang, Brian.E.Carpenter

Stig Venaas

IETF 83@Paris

Mar 2012

Progress

Adopted as a WG item

- *WG Chair initialed the Call in Dec 2011*
- *Submitted as a WG draft in Feb 2012*

Main change since last meeting

- *Individual-to-WG_item revisions*
- *Added a sub-clause of Multicast renumbering issues (Mainly from new co-author* Stig Venaas*)*

Individual-to-WG_item revisions

- Dynamic DNS update *(Modified some technical description. Thanks for* Randal Atkinson's *comments)*

➢ *RFC3007 seems not widely used in internet.*

- We learned that some NICs use VPN to ensure the update [RFC2136] security for customers)

- TSIG/SIG(0) mainly used between DNS server-level, not suitable between hosts and servers, because of the key sharing complexity issue.

➢ *In enterprise, RFC3007 can be easily enabled in integrated systems provided by one vendor (e.g. Microsoft DNS servers & DHCP Servers)*

➢ *Proper mechanism of dynamic DNS records update for normal hosts is still a gap.*

Individual-to-WG_item revisions(cont.)

- A6 is going to be historic (draft-jiang-a6-to-historic, in RFC Queue)

- And some editorial revision

Multicast

- Leave it to Stig Venaas

Next Steps

- Ask for more review
- May expand several topics
  - *DDNS issue*
  - *ACL/Filters bulk update*
  - *Mobile IP relevant*
- Ask for more contributors

Multicast renumbering issue

- Renumbering of *multicast sources*
- Renumbering of *Rendezvous-Point* and *MSDP peers*
- Renumbering of *multicast addresses*

- # Renumbering of multicast sources

- Application on a host may need to be restarted for multicast source renumbering.

- For ASM (Any-Source Multicast) the impact on a receiver is that a new source appears to start sending, and it no longer receives from the previous source. Whether this is an issue depends on the application, but we believe it is likely to not be a major issue.

- For SSM (Source-Specific Multicast) however, there is one significant problem. The receiver needs to learn which source addresses it must join. Some applications may provide their own method for learning sources, where the source application may somehow signal the receiver.

- Otherwise, the receiver may e.g. need to get new SDP information with the new source address. This is similar to how to learn a new group address, see the “Renumbering of multicast addresses” topic below.

- Renumbering of Rendezvous-Point and MSDP Peers

- If the unicast addresses of routers in a network are renumbered, then the RP address is also likely to change for at least some groups
- For PIM-SM one typically switches to SPT (Shortest-Path-Tree) when the first packet is received by the last-hop routers. Forwarding on the SPT should not be impacted by change of IP address. Although one may have to be careful and not unconfigure the previous mapping before configuring a new one, because implementations may revert to Dense Mode if no RP is configured.
- Renumbering of addresses used for MSDP peerings will require peerings to be reconfigured, and be unavailable at least for a brief time.

- Renumbering of multicast addresses

- Unicast-Prefix-based IPv6 Multicast Addresses [RFC3306] and Embedded-RP IPv6 Multicast Addresses [RFC3956]. In that case the multicast addresses used may have to be renumbered.
- When multicast addresses are changed, source applications need to be reconfigured and restarted. Multicast receivers need to learn the new group addresses to join.

Comments?

Thank you

leo.liubing@huawei.com
jiangsheng@huawei.com
brian.e.carpenter@gmail.com
stig@cisco.com

Mar 26-2012, @Paris

Backup

Dynamic DNS Update (DDNS)

- **RFC2136** *Dynamic Updates in the Domain Name System (DNS UPDATE)*

```
(1) Add RRs to an RRset.
(2) Delete an RRset.
(3) Delete all RRsets from a name.
(4) Delete an RR from an RRset.
```

- Normally not directly enabled since there's no secure mechanism in it

Secure Dynamic DNS Update

- **RFC3007** Secure Domain Name System (DNS) Dynamic Update. Specified how to use the following authentication mechanisms:
  - **RFC2535** *Domain Name System Security Extensions （DNSSEC），PKI-based*
  - **RFC2931** *DNS Request and Transaction Signatures (**SIG (0)s**)，RFC2535 relative part update*
  - **RFC2845** *Secret Key Transaction Authentication for DNS (**TSIG**)，shared_key-based*
- **Widely supported by BIND/Microsoft/ Apple .etc**