

Renumbering still needs work

draft-carpenter-renum-needs-work

<http://tinyurl.com/numnum>

Brian Carpenter (U of Auckland)

Ran Atkinson (Extreme Networks)

Hannu Flinck (Nokia Siemens Networks)

January 2009

The idea for this draft came out of discussion about the infeasibility of renumbering in the Routing Research Group. The RRG reached consensus that whatever solution it proposes should not require site renumbering.

But this worries us because...

Renumbering will happen anyway

- As IPv4 addressing enters its end game, address space will be vigorously consolidated, and that inevitably leads to renumbering actions.
- As IPv6 deploys, people will make false starts, need to correct their addressing plans, and that inevitably leads to renumbering actions.

Other reasons for renumbering

- Change of service provider, or addition of a new service provider, when provider-independent addressing is not an option.
- A service provider itself has to renumber.
- Change of site topology (i.e., subnet reorganisation).
- Merger of two site networks into one, or split of one network into two.
- During IPv6 deployment, change of IPv6 access method (e.g., from tunnelled to native) or addressing plan (e.g., PI ↔ PA).

A strategic assertion

- It's important to implement and deploy techniques for IPv6 renumbering, so that as IPv6 becomes universally deployed, renumbering becomes viewed as a relatively routine event.
- In particular, some mechanisms being considered to allow indefinite scaling of the wide-area routing system may assume site renumbering to be a straightforward matter.
- The most demanding case would be unplanned automatic renumbering, presumably initiated by a site border router, for reasons connected with wide-area routing.

Not exactly a new problem

- Am I the only person who inherited a network configured using Sun's default setting in the mid 1980's (1.0.0.0/8)?
 - That made it kind of hard to connect to the Internet
- 1996: "Renumbering Needs Work" [RFC1900]
- 2005: "Procedures for Renumbering an IPv6 Network without a Flag Day" [RFC4192]
 - And quite a few other RFCs in between
- But site renumbering remains a big pain

The network will be down for
cleaning today



Objectives of the draft

Considering both IPv4 and IPv6:

- Summary of existing renumbering mechanisms
- Description of current operational issues with renumbering
- Summary of relevant work in progress
- Gap analysis
- May lead to suggestions for future work, and/or operational recommendations.

Existing Host-related Mechanisms

- DHCP and DHCPv6
 - "Strong" asset management. Site has a central database with MAC addresses, admin info, plug #, and uses this to generate DHCP, DNS, ACLs...
 - "Weak" asset management. No database, FCFS addresses from DHCP, DNS and ACLs maintained manually.
- SLAAC (IPv6 stateless address autoconfig)
 - Hosts inherit subnet prefix from their local router.
 - Designed for unmanaged, unattended automatic configuration.
- PPP
 - IPv4: the server end of PPP assigns subscriber address
 - IPv6: PPP only assigns interface-identifiers. DHCPv6 or SLAAC is used to assign subscriber address.

DNS aspects

- It's elementary that you shorten DNS TTLs before renumbering
- Dynamic DNS and DNSSEC are needed if you want real automation

Existing Router-related Mechanisms

- Router renumbering for IPv6 via DHCPv6 Prefix Delegation [RFC3633]
- ICMPv6 extension to allow router renumbering [RFC2894] (not used??)
- IPv4??

Multi-addressing for IPv6

- IPv6 was designed to allow multiple prefixes per subnet and therefore multiple addresses per host.
- Yes, that has some issues (some glitches in RFC3484 address selection rules, and some issues for exit router selection, ISP ingress address filtering, and traditional TE).
- But it allows overlap between old and new address plans during renumbering. Avoids a flag day.
- Also allows use of ULAs (unique local addresses) for invariant internal addressing (e.g. for network management, printers)

But there's a basic design flaw

- It's obvious that you should shorten address lifetimes prior to renumbering, but
 - IP addresses do not have a built-in lifetime.
 - Even when an address is leased for a finite time by DHCP or SLAAC, or when it is derived from a DNS record with a finite time to live, this information is lost once the address has been passed to an upper layer by the socket interface.
 - Thus, a renumbering event is almost certain to be an unpredictable surprise from the point of view of any software using the address. Many of the issues below derive from this fact.
 - Don't expect this bug to be fixed any time soon.

Operational issues

- Host-related
- Router-related
- Other
 - NAT state issues
 - Mobility issues
 - Multicast issues
 - Management issues
 - Security issues

Host issues

- Network layer *should* do the right thing when DHCP or SLAAC is updated.
 - With "weak" asset management, some confusion seems inevitable, especially around servers.
 - Note that many DHCP options carry addresses around
 - The M/O bit ambiguity in the interaction between DHCPv6 and SLAAC will cause problems during renumbering
 - Embedded systems may need manual or ROM updates
- TCP and UDP sessions break. SCTP might survive.
- DNS - prone to administrative errors and TTL override
- Applications that remember addresses will break.
 - Notorious example: software licences keyed off the IP address.

Router issues

- RFC2072 (from 1997) discusses issues.
 - Some improvement since then (DHCP was still young)
 - Systematic planning and administrative preparation is needed
 - All forms of configuration file and script must be reviewed
 - Addresses are cached in routers - routers may need to be restarted
 - Addresses used by configured tunnels and VPNs may be overlooked

NAT state issues

- Entries in the state table of any NAT that happens to contain renumbered addresses will become invalid before they time out. (Doesn't matter too much, since TCP and UDP break anyway.)
- A NAT itself may be renumbered and may need a configuration change

Mobility issues

- A Mobile IP node will be affected if either its current care-of address or its home address is renumbered.
- Mobile IPv6 will recover *except* if it is disconnected at the moment of renumbering. In that case, it has to use DNS to find its home agent again.
- Mobile IPv4 will not normally recover until the mobile node is back on its home network again.

Multicast issues

- IPv6 multicast actually helps renumbering due to the SLAAC discovery mechanisms.
- However, there are issues due to use of IPv6 unicast addresses in the Rendezvous Point and Source Specific Multicast mechanisms.
- IPv4 multicast: TBD

Management issues (1)

- Static addresses are routinely embedded in configuration files and network management databases, including MIBs.
 - Ideally, all these would be generated from a site asset management database.
- Because of routing policies and VPNs, a site may embed addresses from other sites in its own config data. Thus renumbering will cause a ripple effect for a site's neighbours.
- Some config data may be very hard to find, e.g. configs for building routers, printer addresses configured by individual users, and personal firewall configs.

Management issues (2)

- Use of FQDNs rather than raw IP addresses wherever possible in config files and databases might reduce/mitigate the potential issues.
 - But there's 20 years of history of not doing that.
- Administration issues (i.e., tracking down, recording, and updating all instances where addresses are stored rather than looked up dynamically) are the dominant concern of managers considering the renumbering problem.
- There's a risk element stemming from the complex dependencies of renumbering: it is hard to be fully certain that renumbering will not cause unforeseen service disruptions.

Security issues

- IPv6 addresses are intended to be protected against forgery by SEcure Neighbor Discovery (SEND) [RFC3971]. But SEND appears to be very difficult to actually deploy and operate.
- Firewall rules need to be updated, and any other cases where addresses or prefixes are embedded in security components (ACLs, AAA systems, IDS, etc.)
- Problem if an X.509v3 PKI Certificate includes a subjectAltName extension containing an IP Address.
- Spam white lists need to be updated.
- DNSSEC is needed, to make security folk less nervous about using FQDNs.

Mechanisms in the IETF mill

- SHIM6 - intended to help multihoming, but would also simplify address overlap during renumbering
- MANET (mobile ad hoc networks) - such networks demand automatic addressing and routing setups. Maybe the mechanisms can be generalised? But this work is going very slowly.
- NETCONF - secure remote config
- NSCP (nameserver control protocol) - based on NETCONF

Gap analysis (preliminary) (1)

- Host related gaps:
 - FQDN based socket API or FQDN based transport layer (to alleviate application layer issues)
 - Multipath survivable transport protocol
 - Single registry per host for all address-based configuration
 - IPv4 equivalent of "reconfig-init"?
 - IPv6 ND M/O flag debate to be resolved
 - IPv6 hosts should be able to learn "liveness" of upstream prefixes

Gap analysis (preliminary) (2)

- Router-related gaps
 - A non-proprietary secure mechanism to allow all address-based configuration to be driven by a central repository for site configuration data. NETCONF might be a suitable basis.
 - A MANET solution that's solid enough to apply to fully operational small to medium fixed sites for voluntary or involuntary renumbering.
 - A MANET-style solution that can be applied convincingly to large or very large sites for voluntary renumbering.
 - Short-term, make [RFC2894] and [RFC3633] router renumbering operable.

Gap analysis (preliminary) (3)

- Operational gaps
 - Deploy DNSSEC.
 - Deploy multi-prefix usage of IPv6 (as an aid to renumbering)
 - Document and encourage systematic site databases and secure configuration protocols for network elements and servers (e.g., NETCONF).
 - Document functional requirements for site renumbering tools or toolkits.
 - In general, document renumbering instructions as part of every product manual.

Gap analysis (preliminary) (4)

- Other gaps
 - Secure mechanism for announcing changes of site prefix to peer sites and in public.
 - For Mobile IPv6, better mechanism to handle change of home agent address while mobile is disconnected.

Input requested

- <http://tools.ietf.org/id/draft-carpenter-renum-needs-work>
- Please read the draft, and email your comments (errors, omissions, suggested text)
 - write to the authors, or the ops-area@ietf.org list