IPv6, IPv4 Runout, and v4/v6 Transition Update

Internet Society Standards and Technology Staff Presentation

Phil Roberts

Topics

- IPv6 Organization Member Study
- Observations on IPv4 Runout
- Transition Impacts of Shared Addressing Methods

IPv6 Organization Member Study (Background)

- ISOC has about 90 Organization Members
- Organization Members have great diversity in size, type of organization, geographical location, and operational network types
- During late summer we canvassed our members for information about actual deployment of IPv6 in their operational network
- The results are about to be published in a report here: (http://www.isoc.org/educpillar/resources/ipv6.shtml#other)

IPv6 Organization Member Study (Highlight Observations)

- Respondents varied in IPv4 allocation blocks of from a few addresses to a /8; most of the allocations reported utilization of their address space at around 80%
- Predominant response to the question about what to do when you can't get more space is not to use IPv6 but to use more NAT
- Predominant response to the question about advantages of IPv6 is of course that it has more addresses
- When asked whether an organization would be willing to return any of its IPv4 allocation, almost everyone said "no"
- Response to questions about specific business drivers were pretty vague, but two high runners were 1) needed for IPv6 product development and 2) customer demand
- Specific advice for others interested in deploying IPv6 highlighted the need to start now and the lack of skills and experience in working with IPv6

Observations on IPv4 Runout

- Because transfers will occur, they should be registered
- Registration is required to preserve the integrity of the routing infrastructure
- RIRs are not inclined to operate managed address markets, but need to acknowledge transfers
- Extending availability of IPv4 addresses through transfers could bridge to deployment of IPv6

Importance of registration

- Registration is required to preserve the integrity of the routing infrastructure
- The integrity of the routing infrastructure depends on who can inject routes into the global route table.
- Ongoing problems with illegitimate routes being injected into the global routing infrastructure must be solved.
- We cannot envision any way to solve this without knowing the current legitimate holder of address prefixes.
- The IETF working group on Secure Inter-Domain Routing is considering a routing public-key infrastructure that would rely on valid address holding records.

Impacts of shared addressing methods during transition

- (See Alain's email to IETF behave mailing list Nov 2008)
- Informal discussions with network operators seem to confirm these concerns; eager to hear further operator input confirming or rebutting these concerns
- Mostly impact of address sharing, but there is the "control" element of CGNs in solutions requiring CGNs
- Basic issue is that a large number of subscribers (across households) will be sharing a single IP address

Shared address side-effects

- Ports become a critical resource that must be managed
- Connections to well-known port numbers will need to be reworked
- UPnP doesn't seem to hold-up in this kind of scheme
- "Subscriber" identification semantics will change
  - Used in server apps to protect network (authorization attempts per "subscriber")
  - Other id specific services (such as geolocation, etc.)