IAB Thoughts on IPv6 Network Address Translation

draft-iab-ipv6-nat-00.txt

IAB RFC 4924

Since many of the fundamental forces that have led to a reduction in the transparency of the IPv4 Internet also may play a role in the IPv6 Internet, the transparency of the IPv6 Internet is not pre-ordained, but rather represents an ideal whose maintenance will require significant ongoing effort.

-IAB, July 2007

Thoughts on Problem Space

- **Avoiding renumbering** and **Site multihoming** issues relate to (real or perceived) routing scalability concerns by registries and upstream providers injecting into DFZ
  - NAT generally doesn't support connection failover, load balancing, traffic engineering, etc either
- **Topology hiding** and **Preventing host counting** require further research; translation may or may not be part of a solution
  - Translation is not sufficient to solve them
- **Simple security** is orthogonal to the NAT discussion

Architectural Principles

1. The Internet should accommodate parties having different goals that lead to different practices

2. Non-IPv6-NAT parts of the Internet should not be adversely affected by any IPv6-NAT parts of the Internet
   - Includes operators, developers, and users
   - So the question for IPv6 NAT proponents is how to hide impact within a localized scope

Solution Space

Endpoints get:

A. Global PI addresses
B. Native local, and tunneled global addresses
C. Local addresses, with NAT in the network

A) Global PI addresses

- PI space must be available to all managed networks
- Need to alleviate routing scalability concerns for this to be a viable option
- Ongoing research and experimentation (e.g. LISP)

- If the concerns can be solved in time, would avoid the problems introduced by NAT.

- Doesn’t address topology hiding or host counting

B) Native local, and tunneled global addresses

- Suggested in [RFC4864], e.g. MIPv6
- Physical interfaces get stable local (e.g. ULA) addresses
  - Internal infrastructure thus uses stable prefixes
  - Local communication uses local prefixes
- Tunnel(s) get dynamic global address(es)
  - Global communication uses global addresses
  - Renumbering constrained to systems operating over or beyond the tunnel (e.g. DNS, apps)
    - Those systems can often already deal with changes
- Incentive issues if tunnel endpoints owned by different entities

C) Local addresses, with NAT in the network

- Local communication uses local prefixes
- Global communication gets NAT'ed
- Breaks end-to-end transparency unless translation is reversible (e.g. NAT66), and is reversed by another NAT
  - Incentive issues if the reversing NATs are owned by different entities

End-to-End Transparency

- End-to-end transparency is key to the success of the Internet
- This means immutable fields arrive intact
  - Currently includes source and dest addrs, and are used as such by many protocols and apps
- Each of the 3 classes of solution can be defined to preserve end-to-end transparency

Recommendations

- Consider end-to-end transparency a requirement for any solution

- Compare solutions based on other aspects including scalability and ease of deployment