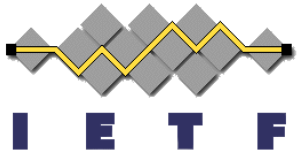
Discovery of a Network-Specific NAT64 Prefix using a Well-Known Name

IETF #82 Behave WG, November 17, 2011



draft-ietf-behave-nat64-discovery-heuristic

Teemu Savolainen, Jouni Korhonen

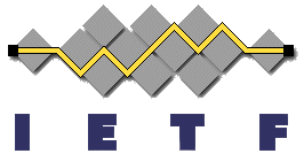
Contents

- Analysis draft status
- Changes in heuristic draft since IETF#81
- Well-known name from Address and Routing Parameter Area (ARPA)?

Analysis draft status

- draft-ietf-behave-nat64-learn-analysis-01.txt
- Through WGLC, now at IESG evaluation
- tsv-dir review received
  - Clarifications about STUN usage and comparison
  - Nits
- No changes in conclusions

Changes in the heuristic draft since IETF#81 (01->03)



- Removal of logic for non-standard addr formats
- RECOMMENDS to go all-IPv6 if possible
- Clarification that separate ”connectivity test” is oftentimes not necessary (just try to connect)
- Well-known name must be signed with DNSSEC – and host SHOULD implement validating DNS resolver, or request the recursive DNS resolver to perform validation. *More on that later.*
- Exit strategy proposal mostly removed
- Significant improvements to security section

Well-known name from Address and Routing Parameter Area (ARPA)?

ipv4only.arpa

- No sub-domains below *ipv4only*
- ARPA zone is signed
- Can be assigned by IETF (RFC3172)
- Public IPv4 address(es) needed for the name (one or more – in case the same bit pattern appears in the NSP as well)
- Quarenteed NOT to have AAAA record

About DNS64 and DNSSEC

- Validating DNSSEC-aware host needs to learn NSP ***securely***, otherwise local AAAA synthesis procedure can be compromised.
- How to accomplish that?

1. Recommending secure channel between host and DNS64 in NAT64 deployments (link layer (e.g. 3GPP network), IPsec, ...)?
2. And maybe additionally: defining some kind of *network supported* heuristics? E.g. finding FQDN of translator via PTR query (of NSP) and validating that with DNSSEC?