DNS Server Selection on Multi-Homed Hosts

draft-savolainen-mif-dns-server-selection-03

Teemu Savolainen (Nokia)
DNSOP WG meeting @ IETF#78
27-July-2010
Advanced multi-homed hosts

- Are connected and using multiple networks at the same time (over WLAN, cellular, VPN..)
- Some of the configured DNS servers may serve non-global information, e.g.
  - Private names for intranet use (e.g. VPN interface)
    - Special case is DNS server having only private information
  - DNS64 synthesized addresses which are only locally valid (e.g. cellular interface)
- Hosts should be able to do forward and reverse DNS queries efficiently

(Note: Microsoft’s Name Resolution Policy Table implements this kind of approach)
Broadband Forum liaison statement

- [https://datatracker.ietf.org/liaison/922/](https://datatracker.ietf.org/liaison/922/) (2010-07-08)
- Quote:”Some IETF efforts that are of special interest to us include:
  - IPv6 multi-homed premises (where the CE router or host is connected to more than one IPv6 service provider); for example, as described in [http://tools.ietf.org/html/draft-troan-multihoming-without-nat66-00](http://tools.ietf.org/html/draft-troan-multihoming-without-nat66-00). Individual technical issues are source address selection policy distribution, route information distribution, and [DNS selection policy distribution](http://tools.ietf.org/html/draft-troan-multihoming-without-nat66-00).
- In BBF’s case different services may be offered on shared IP-connection, e.g. Internet access and sensor networks utilizing private names.
MIF WG work

- DNS resolution issues are already being described in MIF WG document (@IESG):
  - Also in draft-cao-mif-analysis-01

- The proposed solution is being proposed as part of the MIF WG rechartering discussions (current draft):
  - Advanced DNS server selection solution: a specification for describing a way for a network to communicate to nodes information required to perform advanced DNS server selection needed for multi-homing and split-DNS scenarios. The specification shall describe the information to be delivered and the protocol for delivering.
  - Nov 2010: Initial WG draft on DNS server selection solution
  - Nov 2011: Submit DNS server selection solution to IESG for publication as a Proposed Standard RFC
The solution proposal in short

- A new DHCPv6 option to inform nodes (hosts or CPEs) about non-global information a DNS server knows about
- For each DNS query check if some DNS server is known to have special information (matching name suffix or address prefix)
  - E.g. for resolving "server.example.com" use the DNS server known to have non-global information about "example.com"

Note: one implementation alternative is to use indirect hints like information from Domain Search List Options (RFC3646) and from "more specific routes" (RFC4191)
New DHCPv6 option for information delivery

A DNS server address with information it has particular knowledge about:

- DNS suffix(es) (namespace(s))
- IPv6 prefix for reverse lookups

To be added: two bits for preference (like in RFC4191):

- 01 High
- 00 Medium (default)
- 11 Low

- Maybe similar option for IPv4 would be needed
- Preference to be added for selecting the default DNS server
- Maybe suffix field should contain wildcard suffix (e.g. "*") to indicate capability to answer any queries
Request for DNSOP WG

- Confirm client behavior regarding this problem is out of scope for DNSOP WG and it is ok to work on this somewhere else, for example at MIF WG
- Discuss if split-DNS needs to be specified and documented in DNSOP WG
- Solicitation for comments to improve the proposed solution and get terminologies & descriptions perfect