Improved DNS Server Selection for Multi-Homed Nodes

draft-ietf-mif-dns-server-selection-01

Teemu Savolainen (Nokia)

Jun-ya Kato (NTT)

MIF WG meeting @ IETF#80

28-Mar-2011

MIF milestone and overall progress

- 1) 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 at name resolution request granularity in scenarios involving multiple namespaces. The specification shall describe the information to be delivered for nodes and the protocol to be used for delivery.
- *Jan 2011 Initial WG draft on advanced DNS server selection solution – completed*
  - *draft-ietf-mif-dns-server-selection-00 published at 14 January 2011*
- Nov 2011 Submit advanced DNS server selection solution to IESG for publication as a Proposed Standard RFC
  - -01 update uploaded 11 March 2011
  - Feedback to done updates needed as next step

Various changes since IETF#79

- DNS selection option should be included in OPTION_ORO
- DNS server specific route should be created
- Coexistence with RFC3646 clarified
- Refresh Time Option (RF4242) to be used to enable updates outside of general events (e.g. connect/disconnect) ***(-00 -> -01)***

Various changes since IETF#79

- Clarification of which problems are and are not solved
- Deployment scenarios clarification
- Interactions with OPTION_DOMAIN_LIST clarified
- CNAME/DNAME considerations to work with referrals
- Clarifying behavior when multiple options received for the same DNS server, from same or different interfaces

All these changes made between -00 and -01

Security changes since IETF#79

- Clarified possible attack vectors (esp. very targeted attack)
- Added possibility to listen this option only on trusted interfaces and to prefer DNS servers of trusted interfaces even when untrusted interfaces claim higher preference *(-00 -> -01)*
- Added a figure to illustrate node behavior when different interfaces have different trust levels

DNSSEC improvements,-00 to -01

- Node SHOULD implement validating DNSSEC resolver
- A node that accepts DNS server selection rules from non-trusted interfaces and also implements DNSSEC validation SHOULD send queries also to (all) other known DNS servers in case a invalidatable response is received from the preferred DNS server.
- From multiple validated answers the one with preferred trust anchor should be chosen

All these changes made between -00 and -01

Next steps

- IPv4 – is support for that needed?
  - If yes, is it enough to support it via DHCPv6 option?
    - DNS server's IPv4 address as IPv4-mapped address?
    - For PTR queries IPv4 address in in-addr.arpa format?
- Reviews and more comments would be useful
  - Especially from DNSSEC and security point of views
  - To have document ready for WGLC at or after IETF#81