Clarifications on DHCPv6 Authentication <draft-ietf-dhc-dhcpv6-clarify-auth-00.txt>

JINMEI, Tatuya

Toshiba Corporation/The KAME Project

Summary of changes

- Adopted as a wg document
- Proposed resolutions of open issues
  - authentication for Information-request/Reply
  - clarified the definition of "unauthenticated" messages
  - provided a specific suggestion to solve DoS

Authentication for Information-request

- Clarified that auth can be used separately
  - from auth for Solicit/Advertise/Request/Reply...
- Allowed two operation modes
  - tradeoff between securing multiple exchanges and keeping the server "stateless"
  - 1. regard multiple exchanges as a single "session"
    - server keeps per client status
    - perform replay protection
  - 2. separate each exchange wrt authentication
    - MAY skip replay protection
    - client messages may not be authenticated
    - the server can be "stateless"
  - recommend mode 1, but allow mode 2

Definition of "unauthenticated"

- In RFC3315, "unauthenticated" seems to include messages that fail validation
  - => the receiving client could accept such a message
- The proposal: clarify "unauthenticated"
  - msg that does not include an authentication option
  - msg with an authentication option specifying an "unknown" key
  - => now the client MAY accept "unauthenticated" Advertise

DoS protection

- In RFC3315, client MUST restart DHCP on failure of validation
  - => attacker can break a session by simply sending a bogus Reply
- The proposal
  - client still discards the invalid Reply (of course)
  - but waits for a valid Reply until the timeout period expires
    - e.g. wait 1 sec for the initial Request even if it receives an invalid Reply

Next steps

- Resolutions are proposed
- Comments are welcome
  - in particular:
    - Info-req usage
    - DoS protection
- If the proposed resolutions are okay, should be ready for WGLC