Resurrect draft-ietf-dhc-dhcpv6-agentopt-delegate?

IETF-97

Bernie Volz

Last Updated: 11/13/2016 09:30 KST

Background

- Oct 2005 - Ralph, Ole, and Bernie wrote original draft
- Jan 2006, Adopted by WG
- Jan 2009, 04 (last) version published
- Interest was lost because:
  - Out of order packets might cause issues
  - CableLabs specified and relays implemented snooping (WG work was too late)

Motivation

- Avoid relay "snooping" as used in DHCPv4
  - Relay should not need to look inside client's message
  - Security might also make this impossible
- Reduce complexity for relays
  - Some Reply messages do not have details on what client did (i.e., Reply for Release)
- Server provides relay explicit details in Relay-Reply

Design

- Relay added ORO with OPTION_AGENT_NOTIFY to Relay-Forw

- Server added OPTION_AGENT_NOTIFY to Relay-Reply all addresses (IAADDR options) and prefixes (IAPREFIX options) "in use" by client (on link)
  - Valid lifetime used by Relay to track expiration
  - Valid lifetime of 0 meant address/prefix "released"

- Relay no longer needs to look into client's message and is explicitly notified of server actions

So What's The Problem?

- draft-ietf-dhc-sedhcpv6 will encrypt client/server communication so snooping by relays will no longer be possible

So What To Do?

1. Don't allow use of sedhcpv6 when relay needs to snoop (server configuration)
2. Resurrect draft-ietf-dhc-dhcpv6-agentopt-delegate
3. Provide relay server's certificates so it can decrypt
4. Have relay use Active Leasequery (RFC 7653) to keep up
5. Develop Yet-Another-Protocol

Next steps

- Discussion on issue and possible solutions?
  - Which solution does WG favor?
  - Do we want to try (to start) solving this now or wait until sedhcpv6 is further along?
- Resurrect the draft-ietf-dhc-dhcpv6-agentopt-delegate?
  - Do we start with Individual Submission?
  - Or, just republish an 05 as WG document?
- Other comments / questions?