DHCPv6bis Open Issues Discussion

IETF-97

Bernie Volz for DHCPv6bis Coauthors

Last Updated: 11/18/2016 11:10 KST

draft-ietf-dhc-rfc3315bis status

- Jun 2016 – 05 published
- Jul 2016 – WGLC initiated
- Aug 2016 – WGLC ended
  - Approximately 290 comments (some duplicates)
  - 16 serious reviewers (w/multiple comments)
  - THANKS!!!!!!!!
- Oct 2016 – 06 published
  - Addresses about 200 of the comments
  - But more to go!

- While many of the comments are minor
  - Cleanup text / typos / formatting
  - Fix inconsistency issues
  - Clarify sections, definitions
  - Reorganize the text
- We do have a few that are potential changes and require YOUR (WG) input …

SOL_MAX_RT/INF_MAX_RT (19)

- RFC 7083 never stated what happens if multiple Advertise responses are received as to which SOL_MAX_RT (/INF_MAX_RT) should be used
- If client accepts Advertise, should it use option just from that (and ignore others)?
  - What if no option?
  - What if no Advertise accepted?
- Proposal is to use the “smallest” legal value across the received SOL_MAX_RT (/INF_MAX_RT) options
- Probably minor issue as all servers should be configured to use same set of values?

Multiple State Machines (81)

- A request was received to remove text from (05) Section 17.1.10.1:

> Whenever a client restarts the DHCP server discovery process or selects an alternate server, as described in Section 17.1.9, the client SHOULD stop using all the addresses and delegated prefixes for which it has bindings and try to obtain all required leases from the new server. This facilitates the client using a single state machine for all bindings.

- We believe this is to discourage, but allow, running multiple independent state machines on a single interface
- I think we feel that is why it is SHOULD and this text applies to the bindings it obtained under that state machine instance (not necessarily all).

IPsec Encryption Protocol (136)

- In (05) Section 19.1 on Relay/Server IPsec usage, we had a request to remove the NULL protocol:

> The information in DHCP messages is not generally considered confidential, so encryption need not be used (i.e., NULL encryption can be used).

- But then what encryption protocol is used?
- This relates to draft-ietf-dhc-relay-server-security-01 (which was recently WGLC but got no support) … ideally, we could just drop that text here:

> This document recommends combined mode algorithms for ESP authenticated encryption, ESP encryption algorithms, and ESP authentication algorithms as per section 2.1, 2.2, and 2.3 of [RFC7321] respectively. Encryption is recommended as relay agents may forward unencrypted client messages as well as include additional sensitive information, such as vendor-specific information (for example, [CableLabs-DHCP]) and [RFC7839].

Next Steps

- Again, thanks for all that reviewed the document for the WGLC! (If you have comments, it is NOT too late!)
- We’ll continue to work on the list and publish 07 (hopefully with all issues addressed)
- Do a “short” (2-3 week) review to solicit feedback on the changes (or lack thereof)
- Publish 08 if needed
- Send to IESG …